ConCERTO CardMaker Administrator's Manual

Copyright © 2011 SCM Microsystems GmbH

ConCERTO CardMaker
Administrator's Manual
Update: 2011-08-22

Information is this document is subject to change without notice.

Product and company names mentioned herein may be the trademarks of their respective owners.

Direct questions and comments regarding the ConCERTO CardMaker and this document send to concerto@scmmicro.com.

CONTENTS

1 OVERVIEW 7
1.1 Features 7
1.2 Administrator Checklist 8

2 GETTING STARTED 10
2.1 Administrator Software Installation 10
2.2 ConCERTO CardMaker Pre-Installation Checklist 10
2.3 ConCERTO CardMaker Post-Installation Checklist 11
2.4 Client Software Installation 14
2.5 Logon Manager Installation Checklist 14
2.6 Start Program 15
2.7 Card and Reader Configuration 15
2.8 Logon to ConCERTO CardMaker with User Name / Password 15
2.9 Logon to ConCERTO CardMaker with Card 15
2.10 Logoff ConCERTO CardMaker 15
2.11 Exit ConCERTO CardMaker 16

3 CARD ISSUANCE 17
3.1 Issue Cards 17
3.2 Card Printing and Data Layout 19
3.2.1 Verify webcam and printer setup 20
3.2.2 Activate card printing and data layout 20
3.2.3 Make card printing and data layout 20
Issuing photo IDs 23
Self Enrollment 23
3.2.4 To specify a different user group card settings default 24
3.2.5 To specify different user group card settings for different end-users 24
3.2.6 Sample self enrollment scenarios 24
3.3 Temp Cards 25
3.3.1 Issuing temp cards 25
3.3.2 Returning temp cards 26
3.3.3 Additional notes 26
3.4 Add Cardholder 26
3.5 View/Edit Cardholder 26
3.6 Delete Cardholder 27
3.7 Multiple Card Issuance 27
3.8 Fingerprint Reader Usage Notes 27
3.9 Administrator Rights 28
3.9.1 Add Administrator Rights 28
3.9.2 View/Edit Administrator Rights 29
3.9.3 Remove Administrator Rights 29

4 CONFIGURATION 31
4.1 Key File 31
4.1.1 Import Keys 31
4.1.2 Export Keys 31

Copyright © 2011 SCM Microsystems GmbH

4.1.3 Key File Properties 31
4.1.4 Converting Cards from Evaluation to Fully Licensed Keys 32
4.2 Local Settings 34
4.3 Program Settings 35
4.3.1 Application Settings 35
4.3.2 Server Settings 35
4.3.3 Card Printing and Data Entry Settings 37
4.3.4 LDAP/Active Directory Settings 37
4.3.5 Linked Database Settings 37
4.4 Card Settings 38
4.4.1 PIN 39
4.4.2 General 41
4.4.3 Windows Logon 42
4.4.4 Windows Password Policy 44
4.4.5 Website / Application Logon 45
4.4.6 Website / Application Password Policy 46
4.4.7 Backup 46
4.4.8 Server 47
4.4.9 Production 47
4.4.10 Notes 48
4.5 Card Reader Setup 48
4.6 Using Multiple ConCERTO CardMaker Stations 48

5 TOOLS 50
5.1 Data Import 50
5.1.1 ODBC 50
5.1.2 LDAP and Active Directory 51
5.2 Data Export 52
5.3 Schedule Data Synchronization 53
5.4 Logon Entries Wizard 53
5.5 WinLogon Reference Feature 54
5.6 Saving Wizard and WinLogon Reference Entries to Cards 56
5.7 Using Wizard and WinLogon Reference Entries with Managed Entries 57
5.8 Managed Entries 57
5.8.1 Managed Entries Preparation 57
5.8.2 Create Managed Entries 58
5.8.3 Assign Managed Entries with Card Issuance 59
5.8.4 Assign Managed Entries to Cards Which Were Entered or Issued 59
5.8.5 Set Windows credentials 60
5.8.6 Assign Bulk Managed Entries to Cards by Exporting to Excel File 60
5.9 Compact/Repair Database 61

6 SYSTEM MAINTENANCE 62
6.1 Re-issue Card 62
6.2 Self Re-enroll 62
6.3 Report Lost/Stolen/Defective/Returned Card 63
6.4 Identify Card 63
6.5 Update Card Settings 63
6.6 Change PIN 63
6.7 Reset Card PIN 64

6.8 View/Email User PIN/PUK 64
6.9 View/Email Admin PIN/PUK 65

7 BACKING UP, RESTORING, AND UPDATING SYSTEM 66
7.1 Backup All CardMaker Data 66
7.2 Backup Cardholder Data Only 66
7.3 Restore ConCERTO CardMaker Data 66
7.4 Un-installing and Re-installing/Updating ConCERTO CardMaker 67
7.5 Un-installing and Re-installing/Updating ConCERTO LOGON Manager Software 67

8 REPORTS 69
8.1 Cardholders 69
8.2 Pre-entered Cardholders 69
8.3 PIN Letter 69
8.4 Password Letter 69
8.5 Hot-listed Cards 70
8.6 Card Inventory 70
8.7 Transactions 70

9 SUPPORT 71

10 APPENDIX: USING CONCERTO LOGON WITH ACTIVE DIRECTORY 72
10.1Setup to run automated: for users known to Active Directory 72
10.2Setup to run with more control 74
10.3Synchronized Active Directory enrollment 79

11 APPENDIX: USING CONCERTO LOGON WITH TERMINAL SERVICES 82

12 APPENDIX: CUSTOM SCRIPTS FOR CARD REMOVAL EVENTS 83

13 APPENDIX: USING A FAILOVER SERVER 84

14 APPENDIX: CONFIGURING MULTIPLE CARDMAKER STATIONS 85

15 APPENDIX: SSL-SECURED WEBSITE SETUP 86
15.1Open Internet Information Services and Create a Website 86
15.2Setup SSL 88

16 APPENDIX: SSL-SECURED CLIENT SETUP 89
16.1Setup of SSL-Secured Client 89
16.2Install the Certificate Authority's Certificate on the Client Computer 90

17 APPENDIX: DEACTIVATING CARD-SUPPORTED WINDOWS LOGON 92

18 APPENDIX: IMPORT STRING FORMATS 93

Copyright © 2011 SCM Microsystems GmbH

19 APPENDIX: ACTIVE RECORDER APPLICATIONS **96**

20 APPENDIX: BEST PRACTICE FOR WEB /APP DESIGN **97**

1 OVERVIEW

1.1 Features

The ConCERTO CardMaker provides card production and card management capabilities for ConCERTO LOGON Manager Installations.

ConCERTO CardMaker enables Administrators to perform the following tasks:

- Import ConCERTO LOGON Manager License keys into ConCERTO CardMaker program, so they can be used to issue ConCERTO cards.
- Specify card settings, which will govern how end-users use ConCERTO LOGON Manager Program features.
- Issue ConCERTO LOGON Manager cards to end-users, or allow end-users to self enroll.
- Designate certain cardholders as Administrators, and designate different levels of administrator rights within the ConCERTO CardMaker software.
- Re-issue card, or allow cardholders to self re-enroll, when card is lost, stolen, or defective.

Additionally, ConCERTO CardMaker provides the following features:

Convenience

- When contact cards, contactless cards, or other types of tokens are used at the same installation, they can both be managed using the same ConCERTO CardMaker installation.
- Can be synchronized with Active Directory, so that new end-users in Active Directory will be imported into ConCERTO CardMaker on a regular basis, and Windows password changes performed in ConCERTO CardMaker will be synchronized with Active Directory.
- Administrators can define role-oriented "user group" card setting files (such as Administrator, Manager, Secretary…) and use them to create cards with preset defaults for different cardholder groups.
- Administrators can create "user group" managed entries which will be loaded to end-user cards in the specified user group at card issuance, and which Administrator can update while cards are in circulation.
- Card initialization and issuance is accomplished in one simple step, including card printing. ConCERTO CardMaker automatically assigns next available license key to each subsequent card - whether cardholder self-enrolls, or Administrator enrolls cardholder using ConCERTO CardMaker.

Reports

- Cardholder reports, including active and inactive cardholders.
- Hot-list reports for lost, stolen, defective, and returned cards.
- Transaction report recording every transaction which is performed in the ConCERTO CardMaker system, with ID of Administrator who performed transaction. Also shows logon and logoff to Windows for individual cards, as long as the server is activated.
- Card Inventory log showing current card stock.

Card Issuance Options

- **Initialized / Personalized On-site**
  Administrator receives raw card stock from the card manufacturer. Administrator uses ConCERTO CardMaker "Issue Card" commands to load key files, file structure, and card default settings as each card is issued to cardholder, or cardholders use "Self Enrollment" option, which requires no Administrator interaction.

Copyright © 2011 SCM Microsystems GmbH

Secure Processes

- For all data-storing cards: The ConCERTO CardMaker database only stores cardholder enrollment information. All ConCERTO LOGON and personal data is stored on the contact chip.
- For cards which do not store data: The ConCERTO CardMaker database stores cardholder enrollment information, and also functions as a secure data server. ConCERTO LOGON Manager exchanges ConCERTO LOGON and personal data with the ConCERTO CardMaker server in encrypted form, and can additionally be protected by SSL, if desired.
- ConCERTO CardMaker can only be accessed by cardholders who have been granted Administrator rights and who have authenticated themselves with the Administrator password or their ConCERTO card.
- Card-based Administrator rights are stored in a central database and can be granted, changed or revoked immediately and at any time by an authorized Administrator.
- ConCERTO CardMaker ensures that each issued card is secured by its own unique key set for TDES encryption.

1.2 Administrator Checklist

This section provides an overview of the responsibilities of the Administrators. Tasks are listed in logical order, so that the list below can be used as a checklist. Refer to the pertinent manual sections noted, for detailed information on each procedure.

Getting Started

- ❑ Receive, inventory, and acknowledge receipt of all card shipments, license key file shipments (4.1), and ConCERTO LOGON software CDs for the company.
- ❑ Install CardMaker software on one computer (2.1). Windows 2000 Professional or Server, XP Professional, Windows 2003 Server, Vista, Windows 7, or Windows Server 2008 must be installed on computer. Refer to pre- (2.2) and post-installation (2.3) checklists for setup assistance.
- ❑ Install Logon manager software on client computers (2.4 and 2.5).
- ❑ Open ConCERTO CardMaker program and log on with the Administrator password. (2.6)

Configuration

- ❑ If not pre-installed by manufacturer: Import license key files into ConCERTO CardMaker software, in preparation for card issuance. License key files will be provided by the software manufacturer or software distributor via secure email. (4.1)
- ❑ If not pre-set by manufacturer: Configure Local (4.2) and Program Settings. (4.3) For server installations, the Server setting is switched to active by default. Entries required for self enrollment are also specified here. If Windows password changes made by Administrator in the CardMaker software should be synchronized with Active Directory, this option must be switched to active.
- ❑ If not pre-set by manufacturer: Configure User Group Card Setting defaults, as required. (4.4) If a User Group Card Settings file is for a user group that will use server functionality, the server setting must be active.

Prepare for Card Issuance

- ❑ If issuing cards from the ConCERTO CardMaker station:
  Specify card reader which will be used for Administrator logon.
  Specify card reader that will be used for card issuance and maintenance. (4.5)
- ❑ Register card stock, for card inventory log, if desired. (6.11)
- ❑ Import end-user list from Active Directory, or employee database from HR program, if desired. (5.2)

Issue Administrator Cards (if desired)

- ❑ Issue card to self (3.1), assigning self all Administrator rights (3.10). Immediately change card PIN, so that card will be accessible only by self. Store card in secure place, when not in use.
- ❑ Designate additional Administrators as required. If all Administrators will have the same rights, all Administrators can logon to ConCERTO CardMaker with same user name and password. If different levels of Administrator rights are desired, the appropriate level of Administrator rights should be issued to their ConCERTO cards. (3.10)

Prepare Wizard or Managed Entries

- ❑ If system will load wizard or managed entries to the cards of individuals in a specific user group - such as logon information for corporate applications - create the wizard entries and/or a managed entries template card (for server installations). (5.5 and 5.6)
- ❑ If you need to personalize the user name and password for managed entries for individuals, assign managed entries as required (5.6).

Card Issuance and Ongoing Maintenance

- ❑ Issue end-user cards, or allow end-users to self enroll (3.1), and re-issue, or allow end-users to self re-enroll, when cards are lost or defective. (6.1)
- ❑ Issue temp cards (3.4), for use when employees forget their permanent cards at home, if desired.
- ❑ Update user group card settings (4.4) and managed entries information (5.6) as required.
- ❑ Generate reports, as required. (8.0)

Copyright © 2011 SCM Microsystems GmbH

2 GETTING STARTED

2.1 Administrator Software Installation

Install the ConCERTO CardMaker software, using the ConCERTO LOGON CD provided by your distributor. Or, if you have a ConCERTO LOGON Setup CD file, double-click on the "Installation Options.exe" file to start the Installation Wizard.

1. Before installing the ConCERTO CardMaker software, complete all the steps on the ConCERTO CardMaker Pre-Installation Checklist (as shown in section 2.2 below) that are applicable to your installation.

2. Then to install, select the ConCERTO CardMaker option on the ConCERTO LOGON Installation Wizard screen and click on Install button. The Wizard will install all required components on the administrator/server computer, including the ConCERTO LOGON Manager software, the ConCERTO CardMaker software, and your preferred card reader driver.

   Make sure that you are logged on with administrator rights to any target computer where you will install ConCERTO LOGON software.

   For RFID card/server installations: Windows 2000 Server, Windows 2003 Server, or Windows Server 2008 required for full installations. Windows 2000 Professional, XP Professional, Vista, or Windows 7 can be used for evaluation installations.

3. After installation, complete all of the steps on the ConCERTO CardMaker Post-Installation Checklist (as shown in section 2.3) that are applicable to your installation, to complete ConCERTO CardMaker setup.

2.2 ConCERTO CardMaker Pre-Installation Checklist

Before installing the ConCERTO CardMaker software, complete all of the following steps that are applicable to your installation:

All Installations	
✓	**Confirm Internet Information Services (IIS) Installation** Before installing the ConCERTO CardMaker software, you must confirm that Internet Information Services (IIS) is installed and that the features listed below are activated. Confirm/install from Start > Control Panel > Add or Remove Programs (Programs and Features) > Add or Remove Windows Components (Turn Windows Features On or Off). **For IIS5: (XP, 2003...)** Internet Information Services (IIS) * Common Files * Internet Information Services Snap-In * World Wide Web Service **For IIS7 (Vista...)** Internet Information Services + Web Management Tools * IIS Management Console + World Wide Web Services + Application Development Features * ASP * ISAPI Extensions * ISAPI Filters + Health and Diagnostic * HTTP Logging * Request Monitor + Security

	* Request Filtering

Windows Vista Installations	
✓	**De-activate User Account Control setting** If you are installing ConCERTO CardMaker on a Windows Vista machine, you must ensure that User Account Control (UAC) under Control Panel > User Accounts is unchecked in order to install or uninstall the software.

2.3 ConCERTO CardMaker Post-Installation Checklist

After installing the ConCERTO CardMaker software, complete all of the following steps that are applicable to your installation:

All Installations	
✓	**Verify reader driver installation** Installation of a ConCERTO LOGON compatible card reader driver is required for ConCERTO CardMaker operation. For server installations: The card reader can either be physically connected to the server computer directly, or to a terminal which is used to connect to the server in console mode. After installation, it is not necessary to leave the card reader at the CardMaker computer, unless needed.

Server Installations	
✓	**Encrypt IP Address** *Note: If you are evaluating ConCERTO LOGON using "localhost" server mode, with the ConCERTO LOGON Manager and ConCERTO CardMaker software installed on one computer, you can disregard this step.* Note the IP address where the CardMaker software is installed by going to Start > Run. Type in "cmd" and click OK to see the command prompt. Type in "ipconfig" and hit Enter. IP address for server computer will be displayed. Make a note of the IP address, note whether your CardMaker server is SSL secured, and forward via email to your ConCERTO LOGON distributor support contact, or directly to manufacturer at concerto@scmmicro.com. Manufacturer will encrypt the IP address and return a configuration file to you for installation on end-user PCs, and instructions on how to enter into ConCERTO LOGON Manager. Response time is typically a couple of hours during normal business hours (PST). Security note: Be assured that disclosing the IP address does not pose a threat to the system. ConCERTO CardMaker sensitive end-user data is encrypted and can only be accessed externally through a challenge/response handshake which requires the end-user card and PIN.
✓	**Create Virtual Directory** *Note 1: If you successfully created the virtual directory as prompted during CardMaker installation, you can disregard this step.* *Note 2: If you are using SSL, this step is not required. Instead, follow SSL setup instructions in the Appendix.* Go to Control Panel > Administrative Tools > IIS (Internet Information Services). In IIS, right-click on default website, then go to "New" then "Virtual Directory". At the welcome screen, click "Next". When window pops up asking for an alias, enter "rfserver". Click "Next". At website content directory, click on "Browse" and select Program Files > ConCERTO CardMaker > Data. Click "OK" then "Next". At access permissions windows, enable the "Read" and "Run Scripts" permissions. Click "Next" then "Finish".
✓	**Check Firewalls** Ensure that access to ports 80 and 443 are not blocked by any Firewalls.
✓	**Ensure IIS Server Supports ASP Scripts** Windows 2003, Vista, 7 and 2008 Server installations should be aware that the default settings only support ASP.NET scripts, but by default do not support classic ASP scripts. Since ConCERTO LOGON uses classic ASP scripts, support for ASP scripts must be enabled. Below some guidelines on how to install and enable ASP on the different Windows versions:

Installing Classic ASP on Windows 2003 Server
Click on Start > Control Panel > Add or Remove Programs
Select:
- Add/Remove Windows Components
- Application Server
- IIS
- World Wide Web Services
Check Active Server Pages
Click on Start > Control Panel > Administrative Tools > Internet Information Services, and ensure that Web Service Extensions > Active Server Pages is set to Allowed.

Installing Classic ASP on Windows Vista or Windows 7 Client
- Click Start, and then click Control Panel.
- In Control Panel, click Programs and Features, and then click Turn Windows Features On or Off.
- Expand Internet Information Services, then World Wide Web Services, then Application Development Features.
- Select ASP, and then click OK.

Installing Classic ASP on Windows Server 2008 or Windows Server 2008 R2
- Click Start, point to Administrative Tools, and then click Server Manager.
- In the Server Manager pane, expand Roles, and then click Web Server (IIS).
- In the Web Server (IIS) pane, scroll to the Role Services section, and then click Add Role Services.
- On the Select Role Services page, select ASP.
- If the Add Role Services Required by ASP dialog box appears, click Add Required Role Services.
- On the Select Role Services page, click Next.
- On the Confirm Installation Selections page, click Install.
- On the Results page, click Close.

See also
http://learn.iis.net/page.aspx/562/classic-asp-not-installed-by-default-on-iis-70-and-iis-75/

✓ **Modify access permissions (Optional)**

As a part of installation, ConCERTO CardMaker will automatically add the user "Everyone" to the "Security" tab of the ConCERTO CardMaker Data sub-directory. This user "Everyone" is given full access permissions, so that the Internet Information Services (IIS) is able to access the CardMaker database.

After installation you can further restrict access permissions by removing the user "Everyone" from the "Security" tab and replacing it with a user account that is specifically used for authentication of the virtual directory "rfserver", as described below.

Open Windows Explorer. Right-click on folder "..\Program Files\ConCERTO CardMaker\Data". From the menu that appears, select "Properties" then select "Security" tab.

If your "Security" tab is not displayed:
Launch Windows Explorer or My Computer.
Click on Tools at the menu bar, and then click on Folder Options. Click on View tab.
In the Advanced Settings section at the bottom of the list; uncheck the "Use simple file sharing (Recommended)" check box. Click OK.

If "Internet Guest Account" is NOT listed under "Group or user names", click on Edit/Add button. In the "Select Users or Groups" window, click on the "Locations…" button. In the "Locations" window, select the computer that you are working on and click OK.

Back in the "Select Users or Groups" window, click on the "Advanced…" button. Then click "Find Now" button and select the "IUSR_(computer name)" account (the Internet Guest Account for the computer you're working on) and click OK twice.

Back in the "Data Properties" window, verify that the "Internet Guest Account" is listed and highlighted, and that all permissions other than "Full Control" are checked. Then click on the Apply button, and then on the OK button.

Note: Some installations may need to additionally ensure that IUSR… refers to a local account and that it matches the user listed under Internet Information Services.
You can check this in XP/2000/2003 as follows:
Go to Internet Information Services (server name)>Web Sites>Default Web Site. Right click on rfserver>Properties>Directory Security>Edit under Anonymous access… Ensure that Anonymous access is enabled and that the user name matches.
You can check this in Vista as follows:
Go to Internet Information Services (server name)>Web Sites/Sites >Default Web Site>rfserver>Authentication.

	Right click on Anonymous Authentication>Edit and ensure that the user name matches.
✓	**SSL Setup (Optional)** Installations that will be using SSL to protect communication between ConCERTO LOGON Manager computers and the CardMaker server should now refer to the Appendix, which provides assistance with SSL setup for website and client. After successful SSL setup, continue server setup below.

Additional Installation Tips	
✓	**Remote or rack mounted servers** If your server computer is not physically accessible or is a rack mounted system, proceed as follows: Use a local workstation to connect to server via remote desktop in "Console" mode. Install card reader driver on both server and workstation, and plug reader into local workstation. Note that you may have to connect reader to server's USB port initially, to complete driver installation.
✓	**Distributed installation of client software** Ask your distributor for a ConCERTO LOGON silent installation kit. The ConCERTO LOGON Manager setup is based on Microsoft Windows Installer (MSI) and supports MSI Command-Line Options. These options can be especially useful when installing ConCERTO LOGON Manager from a central server onto distributed clients. The following link to Microsoft MSDN website contains information on MSI command line options and their usage: http://msdn2.microsoft.com/en-us/library/aa367988.aspx
✓	**Terminal Services installations** If end-users will access ConCERTO LOGON Manager inside of Terminal Services sessions, then the ConCERTO LOGON Manager software must be installed on the Terminal Services (TS) server computer. This computer must be running Windows 2003 in order to support all of the Terminal Services features and required smart card services redirection capabilities. When ConCERTO LOGON Manager is installed on the TS server, it can be configured to facilitate logon to the Windows session as well as logon to websites and applications. Services are provided based on the successful authentication of the end-user's card, which must be presented to the card reader at the client computer/terminal. See also Appendix: Using ConCERTO LOGON with Terminal Services, for more information. Note that any computer connecting to the server over RDP (Remote Desktop Protocol) will have its smart card services redirected from the client to the host. In this case, the type of card reader driver installed at the server computer must match the client computer card reader.
✓	**Failover server installations** For installations that require a failover server: If your installation requires a failover server, refer to Appendix: Using a Failover Server for additional information.
✓	**De-installation Note for IIS** Before you de-install ConCERTO CardMaker from any computer, you must first exit ConCERTO CardMaker and re-start IIS (Internet Information Services). This is to ensure that the web server is not currently linked to any of the ConCERTO CardMaker components at the time of de-installation.

Copyright © 2011 SCM Microsystems GmbH

2.4 Client Software Installation

Install the ConCERTO LOGON Manager software at the end-user computers, using the ConCERTO LOGON CD provided by your distributor. Or, if you have a ConCERTO LOGON Setup CD file, double-click on the "Installation Options.exe" file to start the Installation Wizard.

Select the ConCERTO LOGON Manager option on the ConCERTO LOGON Installation Wizard screen and click on Install button. The Wizard will install all required components on the end-user computer, including the ConCERTO LOGON Manager software, and your preferred card reader driver.

Make sure that you are logged on with administrator rights to any target computer where you will install ConCERTO LOGON software.

For RFID card/server installations: Windows 2000 Professional, XP Professional, Vista and Windows 7 compatible.

To set the card, reader and operating mode options that will be offered to end-users: At end-user computer, click on Start > All Programs > ConCERTO LOGON Manager > ConCERTO Card and Reader Configuration to select the options that will be displayed for the end-user at that computer. See the Getting Started section of the ConCERTO LOGON Manager manual for more information.

2.5 Logon Manager Installation Checklist

After installing the ConCERTO LOGON Manager software at end-user computers, complete all of the following steps that are applicable to your installation:

Server Installations	
✓	**Enter Encrypted IP Address** *Note: If you are evaluating ConCERTO LOGON using "localhost" server mode, with the ConCERTO LOGON Manager and ConCERTO CardMaker software installed on one computer, you can disregard this step.* Enter encrypted IP address received from distributor into each End-user computer where ConCERTO LOGON Manager software has been installed (see also Encrypt IP Address instruction in previous section).
Windows 2003 Server Installations	
✓	**Configure Security Settings** You must deactivate the "Internet Explorer Enhanced Security Configuration" preset if you want End-users to be able to Auto-record and Auto-fill web logon entries.
Windows Vista Installations	
✓	**Verify User Account Control setting** If you will be using a card to logon to Windows Vista machines: in order for ConCERTO LOGON to be able to redirect the logon to the card, you must uncheck the "User Account Control" setting, under Control Panel > User Accounts, that limits the user's ability to make changes. You must logon as an administrator to change this setting, so that end-user settings accounts will also be redirected. Next, still as an administrator, open Logon Manager and set the Settings > Logon to Windows > Use card to logon… setting to active.

2.6 Start Program

After the ConCERTO CardMaker software has been installed on your computer, open program as follows:

Double-click on the ConCERTO CardMaker icon displayed on your desktop or select ConCERTO CardMaker from the "Start" menu at the bottom left of your Windows desktop screen ("Programs" option).

2.7 Card and Reader Configuration

The first time that the ConCERTO CardMaker software is started, you will be prompted to select the card and card reader that you will be using with ConCERTO LOGON.

If at a later time, you need to change the card and reader selection, you can change the selection under Start > All Programs > ConCERTO CardMaker > Card and Reader Configuration.

Note that if you logged on to your computer with the card, you will not be able to change the card and reader selection within the same session. You must first logoff of that session, and then logon manually, to change the card and reader selection.

2.8 Logon to ConCERTO CardMaker with User Name / Password

To logon to ConCERTO CardMaker with a user name / password:

1. Click on "File" in the menu bar, and click on the "Logon with User Name / Password" selection.

2. When you are logging on to CardMaker for the first time, the initial password is "admin".

   In order to protect the ConCERTO CardMaker data, you should change the password to a unique password by clicking on the Change Password button. A ConCERTO CardMaker password policy governs password selection, for increased security.

2.9 Logon to ConCERTO CardMaker with Card

To logon to ConCERTO CardMaker with a card:

Note: In order to logon to CardMaker with a card, cardholder must have been issued a card (see section 3.1) and provided with Administrator rights (see section 3.6).

Click on "File" in the menu bar, and click on the "Logon with Card" selection.

1. Present your Administrator ConCERTO card to the card reader, as prompted by the CardMaker window.

2. Type in your ConCERTO card PIN (Personal Identification Number), and click on the OK button.

2.10 Logoff ConCERTO CardMaker

You must logoff ConCERTO CardMaker and remove your card from the card reader whenever you step away from your desk, to ensure that system security is not compromised.

To logoff ConCERTO CardMaker:

Click on "File" in the menu bar, and click on the "Logoff" selection.

Copyright © 2011 SCM Microsystems GmbH

2.11 Exit ConCERTO CardMaker

To exit ConCERTO CardMaker:

Click on "File" in the menu bar, and click on the "Exit" selection, or
Click on "X" in top right corner of CardMaker window.

3 CARD ISSUANCE

ConCERTO card issuance is described below.

The "Issue Cards" section describes card issuance when the Administrator personally issues cards to end-users.

The "Card Printing and Data Layout" section describes how to activate the settings to use the photo capture and card printing functionality, as a part of card issuance. You can also use this section to edit the data that is displayed in the "Issue Card" screen.

The "Self Enrollment" section describes how card installations can allow end-users to register with the ConCERTO LOGON server themselves, with no Administrator assistance.

The "Temp Cards" section describes how the Administrator can designate certain cards as temporary cards, which can be used by end-users if they forget their cards at home.

If you want to issue multiple cards at once, which do not need to be linked with an end-user name, refer to the "Multiple Card Issuance" section.

If end-user will use a fingerprint reader for ConCERTO LOGON authentication, refer to the "Fingerprint Reader Usage Notes" section.

Before you begin card issuance it's a good idea to verify that the card reader that you will be using for card issuance has been specified in the "Configuration" menu under "Card Reader Setup" (see section 4.4).

3.1 Issue Cards

Use the following instructions to issue cards to end-users - including regular end-users and Administrators.

Note: If your ConCERTO LOGON license keys have been pre-loaded by the manufacturer and your program and card settings have been preset by the manufacturer, you can issue ConCERTO LOGON rights immediately. If these items have not been pre-loaded, refer to the "Configuration" section to perform these tasks first (see sections 4.1 - 4.3).

If you will be printing photos, names, and/or ID#s on cards as a part of card issuance, refer to the next section "Card Printing and Data Layout" before proceeding.

To issue ConCERTO cards:

1. Click on "Card" in the menu bar, and click on the "Issue Card" selection.

2. If cardholder names have been pre-entered, click on desired entry to highlight the entry, and click on the Select button. Refer to section 5.2 to import employee data from an HR database.

   Or, to enter a new cardholder, click on the Add New button.

   To find a cardholder - by last name, cardholder ID, or card ID - click on the Find button.

   To sort all records - by last name, cardholder ID, card ID, department, card setting, or date issued - click on the Sort button.

   In the detail window, you can type in or change cardholder information, as desired. Refer to description below, and when information has been completed to your satisfaction, click on the Issue button, to issue the card.

   The fields displayed on your Issue Card screen will be determined by your settings, for example, if the Configuration >

Program Settings > Server option is activated; special server-related fields will be displayed. A description of all possible fields is provided below.

Card ID	The entry for Card ID cannot be entered and will be taken from the next available key set.
Cardholder ID *	* Required entry. Cardholder ID specified must be a unique number within the system. If the organization already uses employee IDs or student IDs, ID should be entered in this field. For card installations used in server mode which use employee IDs and which allow card holders to "self enroll" with the ConCERTO server: cardholder can be required to enter employee ID when he self enrolls (see section 4.2.4). Note also that if cardholders are required to enter their cardholder ID (employee / student ID) during self enrollment (specified under Configuration > Program Settings > Server), that entry will populate this field.
Windows / ConCERTO LOGON User Name	(Optional entry: Only displayed if Configuration > Program Settings > Server > "Apply Initial Windows Logon Data" is checked and "Require Windows/ConCERTO LOGON User Name" and "Require Windows Password" are not checked.) Specify Windows/ConCERTO LOGON user name in this field. If a cardholder has multiple Windows user names, it is recommended that the primary Windows user name be specified as the Windows/ConCERTO LOGON user name. If a Windows/ConCERTO user name is entered in this field, cardholders can be required during self enrollment to enter their Employee ID#, and/or Name, to verify their identity. REMOVE THIS PARAGRAPH If no entry is made in this field, and cardholders are required to enter a Windows/ConCERTO LOGON user name during self enrollment, that entry will populate this field. If Administrator enters both Windows/ConCERTO LOGON User Name and Initial Windows Password, a Windows logon entry will automatically be saved to the end-user's card account when that end-user self enrolls, as long as the "Apply Initial Windows Logon Data" option is checked under Configuration > Program Settings > Server. Note: If cardholders always logon to the same domain, then entry of the Windows user name alone is sufficient. However, if cardholders use different domains, it is recommended that the Windows user name be entered in the following format: myaccount@mydomain.com
Initial Windows Password (self enrollment)	(Optional entry: Only displayed if Configuration > Program Settings > Server > "Apply Initial Windows Logon Data" is checked and "Require Windows/ConCERTO LOGON User Name" and "Require Windows Password" are not checked.) Specify initial Windows password in this field. If Administrator enters both Windows/ConCERTO LOGON User Name and Initial Windows Password, a Windows logon entry will automatically be saved to the end-user's card account when that end-user self enrolls, as long as the "Apply Initial Windows Logon Data" option is checked under Configuration > Program Settings > Server.
Initial Windows User Group (self enrollment)	(Optional entry: Only displayed if Configuration > Program Settings > LDAP/Active Directory > "Synchronize Win New User and Password Changes" is checked.) Specify initial Windows user group in this field. If the "Synchronize Win New User and Password Changes" option is checked under Configuration > Program Settings > LDAP/Active Directory then when a Windows User Name and Initial Password are entered into a cardholder's ConCERTO LOGON account, when the end-user self-enrolls, the new user will be added to Active Directory.
ConCERTO LOGON User	* Required entry. If you defined one or more user group card settings under Configuration > Card Settings,

Group *	they will be selectable here. If you did not define any other user group card settings, the standard ConCERTO LOGON default will be used.
Personal information fields…	(Optional entry.) Additional information about the cardholder can be specified as desired. Note also that if cardholders are required to enter a Last Name and First Name during self enrollment (specified under Configuration > Program Settings > Server), that entry will populate this field. If you intend to email PIN/PUK letters to cardholders, you should be sure to enter end-user email addresses.
Remote Access Enabled	This field will only be accessible if the capability has been activated for the installation under Configuration > Program Settings > Server > "Allow for Individual Cardholders". When this checkbox is checked, cardholder will be allowed to access ConCERTO LOGON server without card or card reader. This option should typically be disabled. When Remote Access is required - for example, if user forgot to load ConCERTO LOGON data to laptop before leaving office - Administrator can enable this capability.
Remote Access Allowed From:	Earliest date remote access incident will be allowed for this cardholder.
Remote Access Allowed Until:	Latest date remote access incident will be allowed for this cardholder.
RF Card ID	Displays RF card ID of card.

Note also the following:
If there is no available key set in your ConCERTO CardMaker system: you will need to import key file(s) before you can proceed (see section 4.1.1).

3. The ConCERTO CardMaker will prompt you to present a ConCERTO card to the card reader. Card will be processed, and window will alert you when you may remove the card and deliver it to cardholder.

   Note: If your installation has the Print PIN Letter capability enabled, you can print out a PIN letter for the cardholder under "Reports". This provides cardholder with the default PIN information for his card.

3.2 Card Printing and Data Layout

If you want to print on the card as a part of card issuance, follow the steps described in this section. You can use the default layout provided by ConCERTO CardMaker, and modify it to suit your installation. Or, you can define your own custom layout.

Note also that, using the card printing and data layout, you can custom define the fields that will be displayed in your "Issue Card" screen - whether or not you plan to print cards. As a default, the "Issue Card" screen contains all of the fields displayed in the table shown on the previous pages. Since many installations do not use all of the fields, this provides an opportunity for you to streamline the look of your card issuance screen.

Tips for card printing and layout:
From our experience, we have seen that with card printers, you really do "get what you pay for". If you want to print a simple logo, name, and photo, you should be able to find a card printer that will accomplish this at a reasonable cost. If however, you want to do more complex printing - printing a background image on the entire card, for example -, you

many want to invest in a higher quality, more expensive printer.

RFID cards: Likewise, RFID cards have a coil and a chip hidden inside of the card that can cause the surface to be slightly uneven. Unless you have a high quality, more expensive printer, you may not be happy with the quality of full images printed on the entire surface of the card, and you may instead choose to keep your design simple in order to achieve a clean looking card print.

Be assured that it is possible to find a card printer will give satisfaction for your card design and budget. We recommend that when you purchase your card printer, you tell the vendor specifically how you plan to print and on what type of card, so that they can recommend the card printer that will give you satisfaction.

3.2.1 Verify webcam and printer setup

If you will be printing photos, you will need a TWAIN compatible webcam. Follow instructions provided by the webcam manufacturer for installation of webcam driver.

Likewise, follow instructions provided by your card printer manufacturer to setup and test the card printer. Your card printer control settings can typically be found under Control Panel > Printers. It is important that you use the test program provided with your card printer to verify that card printing works well, before you use the card printer with the CardMaker software.

3.2.2 Activate card printing and data layout

Click on the "Configuration" menu and select the "Program Settings" option. Activate all applicable boxes in the Card Printing and Data Layout section.

Note that the "Card layout" field contains the name "DefaultLayout". This layout provides a basic card layout including placeholders for a logo, a photo, a name and ID #. You can also create your own layout, as described in the next section. Whichever layout name is entered in this field will be the layout which will be used for card printing.

3.2.3 Make card printing and data layout

Click on the "Tools" menu and select the "Card Printing and Data Layout" option, then click on the Open button to select your desired card layout. If you want to start with a default template, click on the "DefaultLayout" selection. If you want to define a new layout, click on the "Add New" button.

Refer to the table below for a description of the fields. Edit the layout as desired, click on the "Preview" button to preview the layout, and the "Save As" button to save the layout under a new name.

Upon saving a new layout, you will be asked if you want to designate this new layout as the default layout which will be used for card printing and data layout. If you choose to designate the new layout as the default, the layout will be displayed in the "Issue Card" screen.

If you want to custom define your "Field Definitions", use section 4 of the screen to do this. You can custom define your fields, even if you are not using card printing, and the result will be displayed in the "Issue Card" screen as long as you designate the new layout as the default. The provided "DefaultLayout" contains all of the fields which by default are displayed in the "Issue Card" screen. You may delete or arrange the fields to best suit your installation as desired. Be sure that you uncheck the "Print" field for any fields which should not be printed to the card.

1. Card and Printer Settings	Layout Name	The name of this card layout.
	Card height / width	Height and width of the card to be printed. Default value is standard sized ID card.
	Card printer	ConCERTO CardMaker will print to whichever printer is specified as the default printer.
	Printing options	The printing options specified in your card printer driver will apply.

	Show chip	When this box is checked, the approximate location of a smart chip on a card will be displayed. This is provided for design purposes only and will not be printed on the card.
2. Background Image	Background image file	The logo or background image that will be printed on the card. File must be in a printable format recognizable by the card printer - typically .jpg, .bmp, .gif, etc. Note that if your image is too big, it may not be able to be loaded. If this is the case, you should downsize your image and try again. If you want more than one background image - for example, a background that covers the card plus a logo in the top corner - you must use a design tool such as Photoshop to merge the images and save them as one image. Although the file is specified here, the background image file itself must be located under Program Files > ConCERTO CardMaker > Images, so that it can be used by the program. Once the file has been copied to that location, simply enter the file name itself into the field.
	Image height / width	The height and width of the background image to be printed on the card. Note that if you want the image to be a particular size, it is recommended that you edit the image to size before adding the image to the layout. Then, you must enter the exact height and width of the image in order for it to appear true to size. Or, you may also adjust the height and width of the image on the card, but it may no longer be true to the dimensions of the original image.
	Image vertical / horizontal offset	Defines how far the image will be printed from the top left corner of the card, vertically and horizontally. Note that for images that bleed over the card, you can enter a negative number.
3. Photo	Photo capture device	The TWAIN compatible webcam that will be used to take photos.
	Photo height / width	The height and width of the photo that will be printed on the card. Once you have your desired size, be careful to not change the ratio of height to width, or your pictures will be distorted.
	Photo vertical / horizontal offset	Defines how far the photo will be printed from the top left corner of the card, vertically and horizontally.
4. Field Definitions	No.	Field number being defined.
	Field name	Specify a recognizable field name. This field name will appear in the "Issue Card" screen. Note that if you leave this field blank, there will be no label for the field in the "Issue Card" screen.

Copyright © 2011 SCM Microsystems GmbH

	Entry type	Select the applicable entry type as follows: Label: Will print a label on the card, as designated in "Field Name". Not related to any ConCERTO CardMaker database fields. Label specified will always be a constant. Useful if you always want to include a label in front of another field, for example, "Department:" Text: Will print the text as specified in the "Database field name". For example, if you specify "Cardholder_ID" under "Database field name", each cardholder's ID will be printed on their card, as long as it is entered in the "Issue Card" screen in the cardholder ID field.
	Entry type (cont.)	Full Name: Select this option to meld the three entry fields of First Name, Middle Name and Last Name, so that they will be printed on the card in a full name format, for example: "Samantha Jones". Note that when you select the Full Name option, the entry fields for First Name, Middle Name, and Last Name will automatically be included in the "Issue Card" screen. This makes it possible for ConCERTO CardMaker to generate the full name from the information entered into those fields. (The inclusion of the Middle Name is optional, but First Name and Last Name must be included). Text [disable]: Use this option for fields where no text may be entered, for example, fields that are automatically entered from the database itself. The "Date Issued" field, for example, is automatically entered from the database. Text [f/m]: Use this option when the only entries that should be made into the corresponding field are f (female) or m (male), for example, if you need a "Sex" field. Text [y/n]: Use this option when the only entries that should be made into the corresponding field are y (yes) or n (no), for example, if you need to indicate if someone participates in a meal plan. Text [len:1...]: Use this option when you want to specify the exact length that an entry in a field must be, for example, if your corporate ID # is 8 digits, you can specify "len:8".. Length from 1 to 50 is selectable.
	Database field name	Select the corresponding database field name. The information that is printed on the card will be the data entered into the corresponding field on the "Issue Card" screen. Note that you can also create your own fields using the following parameters: AuxiliaryText1-5: Each of these five text fields can contain up to 50 characters. AuxiliaryMemo1-3: Each of these three memo fields can contain unlimited text. AuxiliaryBool1-3: Each of these boolean fields must be related to a statement that can be answered by yes or no.

	Default value	Specify a default value, for previewing purposes only, as desired. For example, a possible default value for "Full Name" is "Samantha Jones".
	Print	Check this box if the field should be printed on the card. When this box is checked, the default value specified for this field will be displayed on the card layout above. Click on the "Preview" button to view any updates to the card layout.
	Position on card	Click on the field depicted in the card layout above to move field to desired place on card.
	Font / Size	Specify the font and font size for the field.
	Font Settings	Specify the color, and whether the field should be bold, italic, or underlined. The 6 digit color field must be in "hex color code" or HTML code. If you don't know the hex code for your color, there are many converters online if you search for "hex color code converter".
	Select Field	Move the "Select field" bar to show additional fields.
	New Field / Delete Field	Click on the "New field" button to create a new field, and the "Delete field" button to delete a field. Note that when you create new fields, or change the names of fields, this will be displayed in your "Issue Card" screen. You can define fields as desired, even fields that will not be printed on the card, by unchecking the "Print" box.

Issuing photo IDs

You can now complete card issuance, as described in the previous section. Once "card printing and data layout" has been activated, the card and data layout will be displayed on the "Issue Card" screen.

To take a photo of a cardholder: make sure that the correct webcam device is selected and click on the "Acquire photo" button. Using the webcam screen, capture and select the picture desired.

To clip the photo, use the "hand" icon which will appear, to move the black box on the photo, until the desired area is outlined and click on "Cut Photo to Frame". The dimensions of the black box are definable in the card layout settings under photo height / width.

Click on the "Preview" button to confirm that the card is print ready, and then click on "Print" to print the card.

Self Enrollment

To enable Self Enrollment for card installations, first ensure that the "Allow Self Enrollment" option has been activated in the "Configuration" menu under the "Program Settings" selection in the "Server" tab.

Note: If your ConCERTO LOGON license keys have been pre-loaded by the manufacturer and your program and card settings have been preset by the manufacturer, Self Enrollment can be used immediately. If these items have not been pre-configured, refer to the "Configuration" section to perform these tasks first.

By default, when end-users self-enroll, they will be assigned to the user group card settings "ConCERTO Default", unless you have specified otherwise. The ConCERTO LOGON default settings (ConCERTODefault.ini) do not require PIN or Password Polices, and use an initial PIN and PUK of "12345".

In the program default setting, when end-users self enroll, the information that they enter will populate the ConCERTO CardMaker database. In this case, it is not necessary to make any previous entry for the end-user in the ConCERTO CardMaker database.

If you want to control self enrollment, or pre-enter end-user data in the ConCERTO CardMaker database and have cardholders verify this information in order to self enroll, there are various self-enrollment settings available in the "Configuration" menu under the "Program Settings" selection in the "Server" tab. The last portion of this chapter describes some sample scenarios, to assist you with establishing your desired self-enrollment settings.

If you prefer that end-users receive different user group card settings when they self-enroll, you have two options, described below.

3.2.4 To specify a different user group card settings default

1. Create a user group card settings file that contains your desired security policy settings in Configuration > Card Settings (see "Configuration" section for assistance).

2. Specify this as the user group card settings file that you want to use as a default when prompted, or specify in Program Settings > System settings in the "Default User Group Card Settings File".

After completion of the above steps, this user group card settings file will now be used as the default file for both card issuance and self enrollment.

If you want end-users to also receive managed entries when they self-enroll, you just need to create managed entries for their assigned user group. See also "Managed Entries" section for assistance.

3.2.5 To specify different user group card settings for different end-users

1. Create your desired user group card settings files containing your desired security policy settings in Configuration > Card Settings (see "Configuration" section for assistance).

2. Go to Card > Add Cardholder, pre-enter the end-user information, and specify the user group card settings file for this individual. When end-user self-enrolls, they will be matched to their entry in ConCERTO CardMaker via the Cardholder ID (which for businesses is the Employee ID), Windows/ConCERTO LOGON user name, or RF card serial number, so make sure that the identifying data has been entered correctly.

After completion of the above steps, when the end-user self-enrolls using their identifying data, they will be assigned to the correct user group card settings file.

If you want end-users to also receive managed entries when they self-enroll, you just need to create managed entries for their assigned user group. See also "Managed Entries" section for assistance.

3.2.6 Sample self enrollment scenarios

The settings shown in this section can be manipulated in the "Configuration" menu under the "Program Settings" selection in the "Server" tab.

Settings for the following sample scenarios are displayed below:

- Program default: no administrator involvement
- Program default, plus required windows logon entry
- Windows logon info pre-loaded into cardholder account
- User name taken from Windows logon process; cardholder enters Windows password

1. Program default: no administrator involvement

Administrator: No involvement.
Cardholder: Enters name and Employee/Student ID# at self-enrollment, which populates ConCERTO CardMaker database. Cardholder then saves Windows logon information and other logon information to card account themselves, as desired.

2. Program default, plus required Windows logon entry
Administrator: No involvement.
Cardholder: Enters name and Employee/Student ID# at self-enrollment, which populates ConCERTO CardMaker database. Cardholder is required to enter Windows logon information during self-enrollment. This automatically creates a Windows logon entry for the card account so that cardholder will be logged on to Windows immediately following successful self-enrollment, or, if already in a Windows session, cardholder will be prompted to present card to logon to Windows after next reboot.

3. Windows logon information pre-loaded to cardholder account
Administrator: Pre-loads user name, Employee/Student ID#, Windows user name, and Windows password to cardholder accounts from Active Directory or other 3rd party software.
Cardholder: Enters employee ID# at self enrollment to link card with ConCERTO LOGON account.

Additional considerations of this option:
* Instead of ID#, Name could also be used to verify cardholder's identity. Or, both Employee/Student ID# and Name could be required.
* Note that if you only pre-load Windows user name and Windows password to cardholder accounts this configuration will still work, since entry of user name in the ConCERTO LOGON database is not required, and if no Employee/Student ID# is pre-entered, ConCERTO LOGON will fill the ID field with the Windows user name.
* Refer to Appendix "Using ConCERTO LOGON with Active Directory" for additional information.

4. User name taken from Windows logon process; cardholder enters Windows password
Administrator: No involvement.
Cardholder: Cardholder is required to enter only Windows password during self-enrollment; their Windows user name is taken from the Windows logon process when they booted up the computer. This automatically creates a Windows logon entry for the card account so that after next reboot, cardholder will be prompted to present card to logon to Windows.

3.3 Temp Cards

The self re-enrollment feature, also described under "Self Re-enroll", can be used to issue a temporary card, which can be used by cardholders in cases when they forget or temporarily displace their original card. The self re-enroll and temporary card features are only available for installations which use a card in server mode.

Temporary cards consist of standard card stock that can be optionally printed with a "temp card" graphic and number system, if desired. Administrator gives the temp card stack to the front desk clerk.

If for a given installation cardholders should be able to use temporary cards, note that the ConCERTO CardMaker software must be configured for server mode, and the self-enrollment option (CardMaker > Configuration > Program Settings > Server > Self-enrollment) must be checked and allowed for all cardholders.

3.3.1 Issuing temp cards

1. Employee forgets his card at home or temporarily displaced his card

2. Employee picks up a temporary card at the front desk.

   It is recommended that a procedure be established to track the issuance and return of temporary cards. For example a "Temp Card Sign-out Sheet" can be prepared with four columns in which the following information can be filled in: temp card #, employee name, date card received, and date card returned
   Clerk then selects any temp card from the stack, employee writes temp card number, his name, and date received before taking card.

3. Employee then presents temp card to card reader at any computer within the network where ConCERTO is installed and self re-enrolls by entering, upon being prompted, his user name (ConCERTO LOGON user name / Windows user name) and card PIN of his permanent card. If employee does not know the card PIN of his permanent ConCERTO card, he will not be able to access his data.

   The successful re-enrollment will automatically clear the permanent card from any link to the employee's data and the temporary card takes over the full functionality and data set of the permanent card. If, for example, the misplaced permanent card gets into the wrong hands after the employee has self re-enrolled with a temp card, the permanent card will act like a new card that has not been issued with no association to the employee's personal data.

4. Employee uses temp card in the same way as he had been using the permanent card until he either recovers/finds the lost permanent cards or is issued a new permanent card.

3.3.2 Returning temp cards

Once the employee has recovered his permanent card, he presents permanent card to reader and then self re-enrolls as described under (3) in the section above. This will automatically clear the temporary card from any link to the employee's data, and the employee may return the temporary card to the front desk. The employee can now use his permanent card as before.

The employee should return his temp card only after the successfully self re-enrolled with his permanent card. All personal data will have been removed from the temp card at that point. Depending on customer's policy, employee may then return the temp card to the front desk clerk. Returned cards can then be reused.

In case the employee is not able to recover his original permanent card, he should report the loss to the card administrator and ask for issuance of a new permanent card.

3.3.3 Additional notes

Temp cards take on the temporary identity of employee: After employee has performed self re-enrollment with a temp card, the employee's personal data will be linked to the temp card. The card administrator can detect whether an employee uses a temp card by verifying if the RfCardID shown under that cardholder matches the RfCardID of a temp card. The RfCardID is shown under "ConCERTO CardMaker > Card > View/Edit Cardholder > Select > Cardholder Details", when the "user card printing / custom data entry" under "Configuration > Program Settings > Application" is unchecked.

3.4 Add Cardholder

To pre-enter cardholder information prior to card issuance, click on "Card" in the menu bar, and click on the "Add Cardholder" selection.

A unique cardholder ID must be entered for every cardholder. Refer to the "Issue Cards" section for more information on the entry fields.

Note that if no previous information is entered for cardholders who will "self enroll", the cardholder will initiate the creation of their cardholder record.

3.5 View/Edit Cardholder

To view or edit cardholder information:

1. Click on "Card" in the menu bar, and click on the "View/Edit Cardholder" selection.

2. Click on desired entry and click on the Select button.

3.6 Delete Cardholder

To delete cardholder information, click on "Card" in the menu bar, and click on the "Delete Cardholder" selection.

If you want to be more cautious about which cardholders you delete, you can make cardholders inactive by adding them to the Hotlist before deleting them, to ensure that you do not delete an active cardholder, for example. To do this, click on Card > Add Card to Hotlist and specify that the cardholder's card was lost, stolen, defective or returned.

3.7 Multiple Card Issuance

If you only need to initialize cards for use with the ConCERTO LOGON software, but you do not need to link the cards with individual end-user names, you can issue multiple cards at once.

In this case, you simply need to enter a Cardholder ID range for the number of cards to be issued, into the Cardholder ID field under the Issue Card option. Then, after you click on the "Issue" button, ConCERTO LOGON will prompt you to present the individual cards to the card reader, one after another, for initialization.

To issue multiple cards:

1. Click on Card > Issue Card and click on the "Add New" button.

2. In the Cardholder ID field, enter a Cardholder ID range, which conforms to the following format:
   "xxxx…"-"xxxx…"

   For example, if you want to initialize 100 cards to be used in the Sales department of your company, you can specify:
   "Sales001"-"Sales100"

3. Click on the "Issue" button, and a progress screen will prompt you when to present each card to the card reader for initialization.

Note that the following rules must be followed to initialize multiple cards:
1. Quotes must enclose each ID specified, with a dash in between, and no spaces, as shown above.
2. Number of digits must be the same in both IDs specified.
For example, for cardholder ID range of 1-99, specify "01"-"99".

Up to 30 characters can be entered in the Cardholder ID field. If you are using a constant alpha character set followed by numeric characters, the alpha characters should precede the numeric characters, for example as follows:
"ODS001"-"ODS900"

If you want the Card ID to be included as the first part of the Cardholder ID, you can specify as follows:
"[CARDID]001"-"[CARDID]099"

3.8 Fingerprint Reader Usage Notes

When ConCERTO LOGON is used with a fingerprint reader, the fingerprint authentication replaces, or is used in addition to, PIN entry.

If end-users at your installation will use a fingerprint reader for ConCERTO LOGON authentication, you must first ensure that the Card Setting "Authentication Method" specifies one of the following options:
"Use fingerprint scan."
"Use PIN OR fingerprint scan."
"Use PIN AND fingerprint scan."

When cards are issued with one of these settings, ConCERTO LOGON will automatically prompt end-users to register their fingerprint(s) with first use. For convenience, the ConCERTO LOGON program suggests that the end-user enroll

the index and middle finger of their "non-primary" hand, ie, if end-user is right-handed, they should register the index and middle fingers on their left hand. End-user can feel free to enroll any of his fingers, but then they must remember which fingers they enrolled.

ConCERTO LOGON is set up to enroll two fingerprints from each end-user. The end-user can then use either of those fingerprints for subsequent authentication. The end-user must place each finger on the sensor three times to enroll - this helps to ensure that the captured image is good.

If some end-users have trouble getting a good image with the fingerprint reader, they are advised to moisturize their finger pads. This approach has been found to be very helpful in ensuring good ridge definition for the fingerprint. This approach is advised both for enrollment and authentication, and can also effectively speed up each process.

The ConCERTO LOGON program advises end-users to refer to their administrator if they are not able to successfully enroll their fingerprints. If end-users have tried using moisturizer without success and come to you for assistance, you can also run through the following points with them:

- Plug in the end-user's fingerprint reader or contact chip, and open the ConCERTO LOGON Manager program.
- When enrollment screen appears, ensure that end-user's finger is laid parallel on fingerprint reader and finger pad is pressed securely on sensor.
- Click on Enroll button to start a new enroll attempt until end-user successfully enrolls.

In rare cases, some end-users may however not be able to successfully enroll their fingerprints. In this case, it is advised that this end-user should authenticate with a card PIN. You must then specify the Card Setting "Use PIN." under "Authentication Method" for this user. You can use the "Update Card Settings" under the "Card" option to load this new user group card setting to the end-users card. Then, the next time that the end-user opens ConCERTO LOGON using that card, they will be prompted to choose a PIN.

3.9 Administrator Rights

If you use the Administrator user name and password to logon to CardMaker, all Administrators will have the same rights.

If you want to assign different Administrator rights to different Administrators, you can withhold the user name and password information from your Administrators, assign Administrator rights to their ConCERTO card and require Administrators to logon to ConCERTO CardMaker with their card. This has the additional advantage that CardMaker will keep track of which Administrator performed which function, so you can track it back later.

Instructions for adding Administrator rights to a ConCERTO card, viewing/editing Administrator rights, and removing Administrator rights are included in this section.

3.9.1 Add Administrator Rights

The description below describes how to give Administrator rights to an existing cardholder.

If the person you want to provide with Administrator rights does not yet have a card, you must first issue a card (see "Issue Cards" section).

To assign Administrator rights to an existing cardholder:

1. Click on "Configuration" in the menu bar, and click on the "Add Admin Rights" selection.

2. The Assign Administrator Rights window will be displayed. This window contains a list of all cards which have been issued.

   The black arrow on the left side indicates the currently selected cardholder. To select a different cardholder, click on the grey box to the left of the respective line.

3. Click on the Select button, to edit cardholder information.

   Edit information, referring to description below. Most importantly, you will first need to click on the check-box next to the "Is Administrator Card" setting, to activate the Administrator rights. Before the Administrator rights become active, you must also click on the "active" checkbox, and ensure that the "Expiration Date" is in the future.

   The table below provides a description of the rights which can be assigned to Administrators. Click on the corresponding check-box, to enable a right for an Administrator.

Right	Description
Active	Administrator rights are activated.
Issue Cards	Administrator has the right to initialize (load files to cards) and issue cards.
Re-issue Cards	Administrator has the right to re-issue lost, stolen, defective, or returned cards.
Change PINs	Administrator has the right to allow card PINs to be changed using CardMaker.
Change Configuration Settings	Administrator has the right to change program Configuration settings (program and card settings).
Add Card to Hotlist	Administrator has the right to report cards to the system as being lost, stolen, defective, or returned.
Unlock Hot listed Card	Administrator can unlock hot listed cards which have been locked, if the installation allows for this capability.
Assign Administrators	Administrator has the right to administrate the access rights of other Administrators. Administrator can only grant those privileges, which have been granted to his own Administrator card.
Settle	(Server/Enterprise version) Administrator has the right to perform a batch upload of information to the central server.

3.9.2 View/Edit Administrator Rights

After Administrator rights have been issued, you can view/edit Administrator information as follows:

1. Click on "Configuration" in the menu bar, and click on the "View/Edit Admin Rights" selection.

2. The Administrator Rights window will be displayed. This window contains a list of all Administrator cards.

   The black arrow on the left side indicates the currently selected Administrator. To select a different Administrator, click on the grey box to the left of the respective line.

3. Click on the Select button, to select the desired Administrator. Edit rights, referring to table provided in previous section for additional information.

4. Click on "Save" to save information.

3.9.3 Remove Administrator Rights

To remove Administrator rights from a cardholder:

1. Click on "Configuration" in the menu bar, and click on the "Remove Admin Rights" selection.

2. The Remove Administrator Rights window will be displayed. This window contains a list of all Administrator cards.

The black arrow on the left side indicates the currently selected Administrator. To select a different Administrator, click on the grey box to the left of the respective line.

3. Click on the Select button, to select the desired Administrator.

4. A window will appear, asking you to confirm removal of Administrator rights for this Administrator. Click on the Yes button, to remove Administrator rights.

Copyright © 2011 SCM Microsystems GmbH

4 CONFIGURATION

If pre-configuration has not been performed by the manufacturer, the ConCERTO CardMaker Administrator performs the following configuration steps before issuing cards:

- Imports the license key file into the ConCERTO CardMaker program.
- Configures local and program settings, including installation-specific system and server settings.
- Configures card settings, by creating one or more user group card setting definitions which will be used for card issuance.
- Selects card reader which will be used for card issuance, as required.

A description of each configuration step is provided below.

4.1 Key File

License key files for the ConCERTO LOGON Manager Card software are delivered to the Administrator as a "Keys…mdb" file. Before the Administrator can create cards or card images, the license key files must be imported into CardMaker.

Instructions for exporting keys and key properties are also provided in this section.

Most organizations prefer to complete their testing with evaluation keys (included with evaluation software), then start fresh with full licenses for their rollout. To do this, they delete all cardholders, export all evaluation keys, then import full license keys before beginning card issuance/self enrollment. However, for organizations that want to convert cards with evaluation keys to cards with full licenses, a final section provides assistance with this.

4.1.1 Import Keys

To import license keys:

1. Copy "Keys…mdb" file to "Program Files\ConCERTO CardMaker\Data" file. ("Keys…mdb" file will be sent directly to Administrator via encrypted email.

2. Click on "Configuration" in the menu bar, and click on the "Keys - Import" selection.

3. Click on desired "Keys…mdb" file in selection box, and click on the Open button.

4. The first Card ID and the last Card ID of the key file will be displayed. Click on the OK button, to import keys.

4.1.2 Export Keys

If the hardware configuration of the CardMaker Server is being changed or updated, Administrators may find that they have to export key files.

Also, most administrators export any evaluation keys that they used for testing purposes, before importing full license keys. If you did not export evaluation keys before importing full license keys, you can still export them from your system by selecting them individually. You can recognize evaluation keys by the Card ID syntax "xxxxxxxx98xxxxxx".

To export license keys:

1. Click on "Configuration" in the menu bar, and click on the "Keys - Export" selection.

2. The first Card ID and the last Card ID remaining in the key file will be displayed. Specify a file name and click on the OK button, to export keys.

4.1.3 Key File Properties

Due to their different storage methods, the capability to re-use keys is slightly different for contact cards (which store data

on the card) and cards which are used in server mode (which store data on the server), as follows:

When you…	With Contact Cards (which store data on the card)	With Any Card Used in Server Mode (which stores data on the secure server)
Delete a cardholder record for which a license key has been used (i.e., card has been issued).	No license key is returned.	The license key is returned to the tally of available keys under "Available Records".
Recycle a card for which a license key has been used (i.e., card has been issued).	The license key is returned to the tally of available keys under "Available Records".	The license key is returned to the tally of available keys under "Available Records".
Reissue a card for which a license key has been used (i.e., card has been issued).	A new license key is required.	No additional license key is required; the previous license key associated with the old card is transferred to the new card.

Therefore, if you are using contact cards, and you want to maintain the same number of license keys, you should "recycle" cards whenever possible. Even if you then discard the card itself, the license key is still restored to the system.

To view information about key files that you have imported:

1. Click on "Configuration" in the menu bar, and click on the "Keys - Properties" selection.

2. File properties, including history, of the master key file (KeyMaster.mdb) - which you just imported - will be displayed. Click on the Log button, to view a transaction log. Click on the Close button, to exit the window.

4.1.4 Converting Cards from Evaluation to Fully Licensed Keys

Typically, pilot or demo installations use evaluation license keys in a controlled test environment for a limited period of time for test purposes. Then, when an organization rolls out a ConCERTO LOGON installation, they export all evaluation license keys from CardMaker, import full license keys, and issue cards to all end-users.

If however, some end-users are already working with evaluation license keys, and you want to convert these cards to fully licensed cards, you can follow the instructions below.

Note: You can differentiate between evaluation keys and full license keys, because an evaluation key number sequence always contains a "98" or "99" in the middle as follows:
xxxx xxxx 98xx xxxx. You can view a card's license key number (Card ID) in the cardholder information screen in CardMaker, or in Logon Manager under Help > Session Info.

1. **End-users make a backup of their ConCERTO LOGON Manager Card data.**
   If end-users want to keep using the data that they already saved to ConCERTO they must backup this data in order to use it with the new license key.

   Sample email text to end-users:
   We will be converting our ConCERTO LOGON installation from evaluation licenses to full licenses, which will require that you backup all data saved to ConCERTO LOGON by 5 PM on August 1.
   Backup ConCERTO LOGON data as follows:
   1. Open the ConCERTO LOGON Manager program and click on Utilities > Backup/Restore.
   2. When you complete the backup, be sure to note the file location where the backup is saved, and remember the backup password that you select so that you can enter it when you restore your data after the license conversion.
   Note: Any data which has not been backed up will be lost and must be entered in again after the conversion.

2. **Administrator prepares cardholder database in ConCERTO CardMaker, so cards can be issued again with full licenses.**
   After end-users have completed their backups, Administrator has two options, as described below:

   No administrator interaction option:
   (cards used in server mode only)
   Administrator deletes cardholder records of all end-users whose cards have an evaluation license key. This will enable end-users to self enroll with their existing cards.
   * To delete card holder records: Click on Card > Delete Cardholder, and then select the records that you want to delete.
   Note: After having deleted all evaluation card records, you must proceed to next step, Export Evaluation License Keys and Import Full License Keys, before end-users may self enroll their card.

   Administrator assisted issuance option:
   Administrator physically recycles cards of all end-users whose cards have an evaluation license key. Administrator then issues the same card back to the end-user, using a full license key.
   * If you perform this option, it is recommended that you collect all cards with evaluation licenses and recycle them together. This is because when you recycle a card, the license key from the card is returned to the system.
   Note: You must take care that you do not return any evaluation license keys into a system where you have already imported full license keys.
   * To recycle cards: Click on Card > Recycle Card, and present end-user card to card reader.
   Note: After having recycled all evaluation cards, you must proceed to next step, Export Evaluation License Keys and Import Full License Keys, before issuing cards to end-users.

3. **Export evaluation license keys and import full license keys.**
   After all cards with evaluation license keys have been deleted or recycled, continue as follows:
   * To export evaluation license keys: Click on Configuration > Keys > Export. Specify a file name and click on the OK button, to export keys.
   * To import full license keys: Click on Configuration > Keys > Import. Click on desired "Keys…mdb" file in selection box, and click on the Open button, and then click on the OK button to import keys.
   Note: For more information about keys, see previous sections of this chapter.

4. **End-users self enroll or Administrator issues cards, and end-users load their backup file to card.**
   After full license keys have been imported into the system, Administrator has two options - dependent upon option used in step 2 - as described below:

   No administrator interaction option:
   (cards used in server mode only)
   End-users self enroll with their existing card and restore their backup file to their card. (See also sample end-user "self enroll" and "restore backup file" text below.)

   Administrator assisted issuance option:
   Administrator takes stack of cards that have been recycled and issues cards to end-users.
   * To issue cards: Click on Card > Issue Card, and present end-user card to card reader. Select end-user from listing (they will be listed as having "no card"), and issue card.
   * End-users then load their backup file to their card.
   (See also sample end-user "restore backup file" text below.)

   Sample email texts to end-users to self enroll:
   Conversion of our ConCERTO LOGON installation from evaluation licenses to full licenses is complete. To self enroll with your card:
   1. Open the ConCERTO LOGON Manager program and fill in the required information.
   2. Immediately change your PIN to a code that you can remember, as prompted by the program.

   Sample email text to end-users to restore ConCERTO LOGON data:
   Conversion of our ConCERTO LOGON installation from evaluation licenses to full licenses is complete. To restore

previously backed up ConCERTO LOGON data to your card:
1. Open the ConCERTO LOGON Manager program and click on Utilities > Backup/Restore.
2. Click on the Restore option, and select the backup file that you previously saved, entering your unique backup password.
Note: If you did not backup your ConCERTO LOGON data previously, simply enter the data in again.

4.2 Local Settings

Use the instructions provided below to configure local system and server settings.

Most installations will use the same system and server settings all the time, without needing to change them after they have been initially set up. However when desired, you can save a settings configuration by clicking on the Save button.

Default settings in this screen are standard settings, which will suit most installations and may be left unchanged if desired.

To configure local settings:

Click on "Configuration" in the menu bar, and click on the "Local Settings" selection.

Parameter	Description
Site ID	ID to identify installation site, numeric / alpha-numeric, max 5 digits.
Site Name	Name of installation site.
Workstation ID	ID to identify workstation, numeric / alpha-numeric, max 3 digits.
Server Name	The server specified for ConCERTO LOGON functionality during setup.
Server IP Address	The server IP address specified for ConCERTO LOGON functionality during setup.
Server Path	The server path specified for ConCERTO LOGON functionality during setup.
Database Directory	Directory where the card management system database will be stored.
Image Directory	Directory where program images will be stored.
Card Image Files Directory	Directory where card image files will be stored.
Card Settings Directory	Directory where customized card settings files will be stored.

4.3 Program Settings

Use the instructions provided below to configure program settings.

Most installations will use the same program settings all the time, without needing to change them after they have been initially set up. However when desired, you can save a settings configuration by clicking on the Save button.

Many default settings are standard settings, which will suit most installations and may be left unchanged if desired.

To configure program settings:

Click on "Configuration" in the menu bar, and click on the "Program Settings" selection.

4.3.1 Application Settings

Parameter	Description
ConCERTO Card Reader Setup - Administrator	Card reader which will be used for Administrator logon, as specified in "Configuration" menu under "Card Reader Setup".
ConCERTO Card Reader Setup - Production	Card reader which will be used for end-user card issuance and maintenance, as specified in "Configuration" menu under "Card Reader Setup".
Trans. Log Entries stored (days)	Transaction log entries will be stored for specified number of days (can be viewed in Transaction report).
Card Log Entries Stored (days)	Card log entries will be stored for specified number of days (can be viewed in Card Inventory Log report).
Delete Log File At Startup	Specifies if log file will be deleted at start of program.
Default User Group Card Settings File	Specifies which User Group Card Settings file will be offered as the default when editing Card Settings from the Configuration menu. Will also be used as the default for card issuance - for both manual issuance and self-enrollment - when no other User Group is specified.

4.3.2 Server Settings

Parameter	Description
Use Server Functions	Checked: Server functions are available for use. This setting must be activated for all server functionality, including hotlist and card logon events. Not Checked: Server functions not available.
Allow Self Enrollment	Checked: Cardholders can register with ConCERTO LOGON server themselves using their ID card and the ConCERTO LOGON Manager installation at their PC, requiring no Administrator intervention. Not Checked: Cardholder may not self enroll.
Allow Only for Known Cardholders	Checked: Only end-users who are already listed in the cardholder list will be allowed to self-enroll. Not Checked: Any cardholder may self enroll.
Card Serial Number must be within Specified Range	Checked: Only cards that have card serial numbers that fall within a specified range will be allowed to self enroll. The permitted range can be specified under Configuration > Progam Settings > System > Identification. Not Checked: Any cardholder may self enroll.
Require Name	Checked: Cardholder must enter name to register with ConCERTO LOGON server. Not Checked: Cardholder not required to enter name to register with ConCERTO LOGON server.

Require Employee/Student ID	Checked: Cardholder must enter Employee/Student ID to register with ConCERTO LOGON server. Not Checked: Cardholder not required to enter Employee/Student ID to register with server.
Assign Windows User Name as ConCERTO LOGON User Name	Checked: The Windows user name, including the domain if applicable (in the format UserName@Domain), of the currently logged-on user will be pre-assigned as default ConCERTO LOGON User Name. Not Checked: No ConCERTO LOGON User Name will be pre-assigned.
Require Windows/ConCERTO LOGON User Name	Checked: Cardholder must enter Windows/ConCERTO LOGON user name during self enrollment. If a cardholder has multiple Windows user names, it is recommended that the primary Windows user name be specified as the Windows/ConCERTO LOGON user name. If a Windows/ConCERTO LOGON user name for this cardholder has already been entered into the system, the entry will be verified during self-enrollment. If a Windows/ConCERTO LOGON user name for this cardholder does not exist in the system, the entry will populate the database and be saved to the cardholder's ConCERTO LOGON account, as long as the "Apply Initial Windows Logon Data" box is also checked. If cardholders always logon to the same domain, then entry of the Windows user name alone is sufficient. However, if cardholders use different domains, it is recommended that the Windows user name be entered in the following format: myaccount@mydomain.com Not Checked: Cardholder is not required to enter Windows/ConCERTO LOGON user name.
Require Windows Password	Checked: Cardholder must enter Windows password during self enrollment. The Windows password entry will be saved to the cardholder's ConCERTO LOGON account, as long as the "Apply Initial Windows Logon Data" box is also checked. Not Checked: Cardholder is not required to enter Windows password.
Apply Initial Windows Logon Data	If this box is checked, and one or both of the boxes above it are also checked: Upon self enrollment, when cardholder is prompted to enter Windows/ConCERTO LOGON user name and/or password, the Windows logon data will be saved to the cardholder's ConCERTO LOGON account. If this box is checked and neither of the two boxes above it are checked: Upon self-enrollment the initial Windows logon data from the cardholder database record will be assigned to the card. Initial Windows logon data can be entered under menu item "Card > Add Cardholder". These fields will only be displayed and available for data entry in the "Issue Card" screen under these conditions.
Self Re-enrollment only Allowed for Hot listed Cards	Checked: In order for end-user to self re-enroll, Administrator must first report their original card to the ConCERTO system as lost, stolen, damaged or returned - which places the card on the "hotlist". Then, the end-user can take their new ID card, self re-enroll with the system, and recover their previous ConCERTO data to their new card. See also section 6.2. Not Checked: Card must not be hot listed to self re-enroll.
Allow Remote Access Mode for Individual Cardholders	Checked: Individual cardholders who have been granted remote access rights in their cardholder record are permitted to logon to the ConCERTO LOGON server without a card and card reader. For security reasons, this option is typically not activated. Note: this option must be activated in order for the setting in the individual cardholder record to be functional. This double requirement is intended to ensure that this option is used with care. Note also that when Remote Access Mode is activated, any card removal setting will be ignored. Not Checked: Remote Access Mode not allowed, even if Remote Access Mode permission has been granted in individual cardholder record.
Security Override: Disable Laptop Mode	Checked: Cardholders may not save data to Laptop Mode. Even if Card Settings allow Laptop Mode, this universal setting allows the server to override that setting. Not Checked: Laptop Mode settings function as defined in Card Settings file.
Security Override: Require Card in Laptop Mode	Checked: Cardholders are required to use a card and card reader in Laptop Mode. Even if Card Settings allow Laptop Mode without a card, this universal setting allows the server to override that setting. Not Checked: Laptop Mode settings function as defined in Card Settings file.

RF Card Serial Range Mask	8 byte (= 16 hex pairs) code. The mask code is used to specify the bits of the 8 byte card serial number that are to be matched against the Card Serial Range Code. Can be activated to allow only cards in specified range to self-enroll under Configuration > Program Settings > Server > Self Enrollment.
Card Serial Range Code	8 byte (= 16 hex pairs) code. Specifies the part of the card serial number that must have the same value for all cards of the installation. For example, the Card Serial Range Code can be a site or customer code for a given card type. Can be activated to allow only cards in specified range to self-enroll under Configuration > Program Settings > Server > Self Enrollment.

4.3.3 Card Printing and Data Entry Settings

Parameter	Description
Use card printing / custom data entry	Box must be checked if you will be using the photo capture and card printing functionality.
Card layout / custom data entry	The name of the card layout / custom data entry form. A default layout is included.
Enable photo capturing	Box must be checked in order to perform photo capturing with a web cam.
Enable card printing	Box must be checked in order to perform card printing with an attached card printer.

4.3.4 LDAP/Active Directory Settings

Parameter	Description
Synchronize Win New User and Password Changes	Checked: When a Windows User Name and Password are entered into a cardholder's ConCERTO LOGON account, when the card is issued or end-user self-enrolls, the new user will be added to Active Directory. Or, when importing credential file with changed passwords for Windows logon entries, or when changing Windows passwords in the Assign Managed Entries window, password changes will be applied to an LDAP directory (ie, Active Directory). Not Checked: Windows password changes as described above will not be applied to the LDAP directory.
LDAP Connect String	Example for syntax: LDAP://[domain controller]:389/CN=Users,DC=[domain],DC=com
Directory Administrator Name	User name with administrative rights for LDAP directory.
Directory Administrator Password	Password for above user with administrative rights.

4.3.5 Linked Database Settings

This tab will only need to be filled with information when the system is connected to an external linked database, for example, such as an access control system. Please refer to your reseller to find out about ConCERTO LOGON compatibility with access control systems and other centrally managed user authentication systems.

Parameter	Description
Server Name	Server name of linked database.
Database User Name	User name for linked database.
Database User Password	Password for user of linked database.

4.4 Card Settings

The options under Card Settings are grouped under eleven tabs as shown below. The card settings options allow the Administrator to customize how the card PIN is controlled, ConCERTO LOGON Manager Default settings and production settings.

	card settings tab
Customize PIN setting:	PIN
Customize ConCERTO LOGON Manager default settings:	General
	Windows Logon
	Windows Password Policy
	Website / Application Logon
	Website / Application Password Policy
	Backup
	Server
Customize production settings:	Production
	Notes

To configure card settings:

Click on "Configuration" in the menu bar, and click on the "Card Settings" selection.

You can define role-oriented user group card settings (such as Administrator, Manager, Secretary…), by checking/un-checking parameters in the card settings tabs and saving the configuration with a recognizable name, such as "Manager.ini". When you issue cards, you can then select the desired user group card setting default file. The result will be cards which provide customized card features for different cardholder groups.

A file "ConCERTODefault.ini" containing end-user default settings has been provided. This provides a good, basic setting which can serve as a starting point for most ConCERTO LOGON installations. The "ConCERTODefault.ini" file cannot be changed, but changes to the file can be saved under another name.

To create a new default setting file, click on the Save As button and type in a new name. Note that the file ending must be ".ini" for the program to recognize it.

To change an existing card setting file, click on "Open" and select the file in the "Select Configuration File" window. After changing the displayed settings, click on the Save button to save the changes.

If you make a new user group card settings file and you want it to be the default which will be displayed each time you access the "Card Settings" menu and when you issue cards (or when end-users self-enroll), you will be provided with that option when you save the file. Or, you can specify this in the "Configuration" menu in the "Program Settings" menu under the "System" tab.

Refer to the ConCERTO LOGON Manager User's Manual, for more information about the individual card settings.

The options in each card setting tab are described in the tables below.

4.4.1 PIN

Parameter	Description
Authentication Method	Use PIN. End-users will be prompted to enter PIN for authentication. Use fingerprint scan. Fingerprint reader containing a SIM sized contact chip card will be used for authentication. Use PIN OR fingerprint scan. End-users will be prompted to authenticate themselves via the fingerprint reader, but they can click on Cancel button to enter PIN instead. Use PIN AND fingerprint scan. End-users will be prompted to authenticate themselves via the fingerprint reader, then they must additionally authenticate themselves by entering a PIN. No PIN entry. End-users will not be required to enter PIN.
PIN/PUK Assignment Method	Use default PIN/PUK (12345). Cards will be assigned an initial ConCERTO PIN and PUK of 12345. Generate random PIN and random PUK. *(Not available for cards that self enroll.)* Cards which are issued from CardMaker will be assigned a randomly generated initial ConCERTO PIN and PUK. Randomly generated PIN/PUK will be governed by PIN Policy (see below), if activated. To provide cardholder with his random initial PIN and PUK: - Email the PIN/PUK under Card > View/Email User PIN/PUK. You can setup ConCERTO to mail to all new cardholders, or to mail to an individual, or - Print out the PIN Letter, from the "Reports" menu and deliver it to the cardholder. Note for cards running in server mode: Random PIN setting will not be applied to cards which "self enroll", because with self enrollment the cardholder initiates creation of the cardholder record and the PIN cannot be previously specified. See also section 3.2. Use default PIN and admin-managed random PUK. *(Not available for cards that self enroll.)* Cards which are issued from CardMaker will be assigned an initial ConCERTO PIN of 12345 and a randomly generated PUK. PUK which will be known to the administrator and the cardholder cannot change the PUK. - Administrator can view the PUK to unlock end-users cards under Card > View/Email User PIN/PUK, or - Administrator can email the PUK to the cardholder if required under Card > View/Email User PIN/PUK. Randomly generated PUK will be governed by PIN Policy (see below), if activated.
Prompt to Change Default PIN	Remind cardholder to change default PIN with each entry until changed. Cardholder will be prompted to change default PIN, but will not be required to do so. Require cardholder to change default PIN with first entry. Cardholder will be prompted to change default PIN. If cardholder does not change PIN, ConCERTO program will not continue.
Use Second Card PIN (PUK)	A cardholder uses a PUK to unlock their ConCERTO card is they forget their PIN. See also ConCERTO LOGON Manager manual, for more information. Checked: A second card PIN, a PUK, will be assigned to each card. Depending on PIN Assignment Method specified above, the initial PUK will be "12345" or a randomly generated code. When a PUK is used, it will be governed by whatever policies are defined for the use of the PIN. When an the initial PUK is randomly generated, it will also be provided in the PIN Letter, as described above. Not checked: No second card PIN will be assigned.
PIN Verification Timeout	Define how long the PIN will be stored in memory before user is prompted to re-enter PIN. Enter number, in seconds. Entry of "0" =always. Number entered in this field will be displayed as default setting in the PIN Verification Timeout setting in the ConCERTO LOGON Manager software (see

	ConCERTO LOGON Manager General Settings).
Allow Edit of PIN Verification Timeout	Checked: End-users can change the PIN Verification Timeout setting (in ConCERTO LOGON Manager General Settings). Not checked: End-users cannot change the PIN Verification Timeout setting (in ConCERTO LOGON Manager General Settings).
Biometric Security Level	Select sensitivity setting for the biometric matching process from the pull-down menu. The security levels run from lowest security/sensitivity (3) to highest security/sensitivity (10) as follows: Lowest security 3 Medium security 4 Medium security 5 Medium security 6 High security 7 (Program default) High security 8 High security 9 Highest security 10 The higher the setting, the harder it will be to match the fingerprint, which may cause more fingerprints to be rejected. The setting can be adjusted as required for the majority of the end-users. Our recommendation for dealing with end-users who have a harder time authenticating with their fingerprint: • Simply create a separate ConCERTO LOGON User Group for end-users who have trouble authenticating with their fingerprints and require a lower, less sensitive setting, naming the group for example "Trouble Fingerprints". • Set the biometric security level for this group to a level where these users are successful matching their fingerprints, for example, perhaps "5" or "4", and save the User Group settings file by clicking on the Save As button. • Then, re-issue cards to these users using the "Trouble Fingerprints" User Group. Creating a separate User Group for the trouble fingerprints then enables you to keep the default setting of "7" as the general setting for most users. The sensitivity levels correlate to FAR (False Acceptance Ratio) as follows: 3 = FAR 1 in 1,000 4 = FAR 1 in 5,000 5 = FAR 1 in 10,000 6 = FAR 1 in 50,000 7 = FAR 1 in 100,000 8 = FAR 1 in 250,000 9 = FAR 1 in 500,000 10 = FAR 1 in 1,000,000
Allow Edit of Biometric Security Level	Checked: End-users will be able to adjust the level of the biometric security/sensitivity. Not checked: End-users will not be able to adjust the level of the biometric security/sensitivity. Note: In most cases, administrators will prefer to not allow end-users to edit this setting, in order to maintain a high level of authentication security.
PIN Policy Monitoring	Do not monitor cardholder PIN selection according to PIN Policy. Cardholder PIN selection will not be governed by a PIN Policy. Monitor cardholder PIN selection according to PIN Policy. Cardholder PIN selection will be governed by PIN Policy (see below).
PIN Policy	Specify required parameters for cardholder PIN. Choose "x", if you do not want to include that parameter in your PIN. PIN Policy also governs random PIN generation. With random PIN generation, the Max. PIN Length will specify the PIN length.

4.4.2 General

Parameter	Description
Automatically Start Logon Manager	Checked: ConCERTO LOGON Manager program will automatically start after power-up. Not checked: ConCERTO LOGON Manager program will not automatically start after power-up.
Allow Edit of Automatically Start Logon Manager	Checked: End-users can change the Auto-start setting (in ConCERTO LOGON Manager General Settings Option). Not checked: End-users cannot change the Auto-start setting (in ConCERTO LOGON Manager General Settings Option).
Start Minimized	Checked: ConCERTO LOGON Manager program will immediately minimize to system tray (bottom right corner of screen) after power-up when Auto-start is selected. Not checked: ConCERTO LOGON Manager program will not immediately minimize to system tray after power-up when Auto-start is selected.
Allow Edit of Start Minimized	Checked: End-users can change the Start Minimized setting (in ConCERTO LOGON Manager General Settings Option). Not checked: End-users cannot change the Start Minimized setting (in ConCERTO LOGON Manager General Settings Option).
Allow Pop-Up	Checked: ConCERTO LOGON Manager program pop-up capability is enabled so that the ConCERTO programs can automatically pop-up at website and application locations which end-user specifies (in Enter Logon Information window under Pop-up option). Not checked: Pop-up option is not enabled.
Allow Edit of Pop-Up	Checked: End-users can change the Enable Pop-up setting (in ConCERTO LOGON Manager General Settings). Not checked: End-users cannot change the Enable Pop-up setting (in ConCERTO LOGON Manager General Settings).
Disable Logon Manager Application	Checked: The password management part of the ConCERTO LOGON Manager program will not be available to the end user, and the ConCERTO LOGON icon will not be visible in the system tray. However, ConCERTO LOGON to Windows logon functionality will still be available. Administrators or special applications can still launch the Logon Manager program with the following command: ConCERTO.exe /ADMIN Not checked: All ConCERTO LOGON Manager capabilities will be available to the end user.
Disable Laptop Mode (server mode)	For installations which save ConCERTO LOGON data to the server: Checked: Users will not have the option to use the Laptop Mode. Laptop Mode stores ConCERTO LOGON data locally on a laptop so that end-users can access their ConCERTO LOGON data when their computer cannot connect to the ConCERTO CardMaker server over a network connection, for example, when traveling. Not checked: ConCERTO LOGON Manager users will have the option to save data to Laptop Mode.
Require Card in Laptop Mode (server mode)	For installations which save ConCERTO LOGON data to the server: Checked: Users are required to use a card and card reader in laptop mode. By default, it is recommended while traveling that end-users continue to use their card and reader for authentication, since this provides strong security. Not checked: A card and card reader are not required in laptop mode. End-users will be prompted to simply enter their Windows/ConCERTO LOGON User Name and PIN to access data in laptop mode.
Automatically Save Data to Laptop (server mode)	For installations which save ConCERTO LOGON data to the server: Checked: This setting enables cardholders to switch between server mode and laptop mode without having to save the data before they disconnect from the network. When the box is checked, data will always be replicated in both places.

	Not checked: Data will not be automatically saved to laptop mode.
Allow Edit of Automatically Save Data to Laptop (server mode)	For installations which save ConCERTO LOGON data to the server: Checked: Users are required to use a card and card reader in Laptop Mode. Not checked: A card and card reader are not required in Laptop Mode.

4.4.3 Windows Logon

Parameter	Description
Use Card-enabled Logon to Windows	Checked: Default will be set for logon to Windows with ConCERTO card. (Most suitable when logon to Windows entry is pre-set during card initialization.) Not checked: Default will not be set for logon to Windows with ConCERTO card. (Best choice if users will be entering in Windows logon information themselves.)
Allow Edit of Card-enabled Logon	Checked: End-users can change default setting (above) of card-enabled logon. Additionally, Administrator must change the "Permissions" on each local computer, in order to enable the right for cardholders who have only "user" rights to change this setting locally. See instructions provided at the end of this section. Not checked: End-users cannot change default setting (above) of card-enabled logon.
Allow to Bypass Card Logon	Checked: If ConCERTO LOGON Manager is set for logon to Windows with smart card, end-users may cancel the card-based logon process and logon to Windows manually (recommended). Not checked: If ConCERTO LOGON Manager is set for logon to Windows with ConCERTO card, end-users may not cancel the card-based logon process.
Log Card Logon Events	Creates log entry for each end-user Windows logon, logoff, lock, and unlock event. Checked: Card enabled Logon to Windows events will be written to a log and can be viewed under Reports > Transactions. Note also that for smart cards, when data is stored on the card, you must ensure the "Use Server Functions" under Configuration > Program Settings > Server is also enabled. Not checked: Card enabled Logon to Windows events will not be written to a log.
When Card Removed from Reader	No Action If user pulls card from card reader, no action will be taken. Logoff User If user pulls card from card reader, ConCERTO LOGON program will begin countdown, after which Windows will logoff user. Lock System If user pulls card from card reader, Windows will lock system after countdown delay. Shutdown System If user pulls card from card reader, ConCERTO LOGON program will begin countdown, after which Windows will shutdown. Logoff User (TS) Note: Also use this selection if you use a non-PC/SC card reader and you want this functionality. For installations where ConCERTO LOGON Manager runs on a Terminal Services application server: If user pulls card from card reader, ConCERTO LOGON program will begin countdown, after which Windows will logoff user. Lock System (TS) Note: Also use this selection if you use a non-PC/SC card reader and you want this functionality. For installations where ConCERTO LOGON Manager runs on a Terminal Services application server: If user pulls card from card reader, Windows will lock system after countdown delay. Disconnect System (TS) For installations where ConCERTO LOGON Manager runs on a Terminal Services application server: If

	user pulls card from card reader, a disconnect of the remote session is triggered. User can later pick that session up at the same or a different location. Shutdown System (TS) Note: Also use this selection if you use a non-PC/SC card reader and you want this functionality. For installations where ConCERTO LOGON Manager runs on a Terminal Services application server: If user pulls card from card reader, ConCERTO program will begin countdown, after which Windows will shutdown. Custom Script 001 + Disconnect System (TS) For installations where ConCERTO LOGON Manager runs on a Terminal Services application server: If user pulls card from card reader, a custom script will be launched (see Appendix for more information about using custom scripts) and a disconnect of the remote session is triggered. User can later pick that session up at the same or a different location. Custom Script 002… If user pulls card from card reader, a custom script will be launched (see Appendix for more information about using custom scripts).
Use Tap in / Tap out Behavior	Typically used for cards used in server mode, especially contactless cards. When this box is checked, the action that was selected above will be triggered upon tapping the card on the card reader.
Allow Edit of Card Removal Behavior (contact cards)	Checked: End-users can change default setting of card removal behavior (above). Not checked: End-users cannot change default setting of card removal behavior (above).
Countdown Time in Seconds (contact cards)	Define countdown time before action is taken. Enter number, in seconds. Number entered in this field will be displayed as default setting in the Card Control countdown setting in the ConCERTO LOGON Manager software (see ConCERTO LOGON Manager Logon to Windows Settings).
Allow Edit of Countdown Time (contact cards)	Checked: End-users can change default setting of countdown time (above). Not checked: End-users cannot change default setting of countdown time (above).

Additional Instructions: Allow Edit of Card-enabled Logon
(Change "Permissions" on local computers)

Follow the instructions provided below if you want to allow ConCERTO LOGON Manager Cardholders who do not have "Administrator" rights to their computer to change the "Card-enabled Logon to Windows" setting.

1. First, make sure that you are logged on to Windows on the local computer as "Administrator". Ensure that ConCERTO LOGON Manager is closed.
2. In XP or 2000: Click the "Start" button and choose "Run..."
   In Vista: Click on "Start" button, and in "Start Search" field enter "regedit" and click "OK".
3. Under Windows™ XP, enter "regedit" and click "OK".
   Under Windows™ 2000, enter "regedt32" and click "OK".
4. Expand the target Registry tree and single-click/select target key:
   For XP or 2000:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
   For Vista:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers
5. Under Windows™ XP or Vista, right-click on the target key and select "Permissions"…
   Under Windows™ 2000, click on the target key and select the "Security / Permissions..." menu item.
6. Select "User" and Check the "Allow Full Control" check box and click "OK"…
7. Exit the registry editor.

4.4.4 Windows Password Policy

Parameter	Description
Prompt to Change Password Every x Days (0=never)	Define how often cardholder should be prompted to change Windows password. Enter number, in days. Number entered in this field will be displayed as default setting in the ConCERTO LOGON Manager software (see ConCERTO LOGON Manager Logon to Windows Settings).
Allow Edit of Change Password Prompt	Checked: End-users can change the Change Password Prompt setting (in ConCERTO LOGON Manager Logon to Windows Settings). Not checked: End-users cannot change the Change Password Prompt setting (in ConCERTO LOGON Manager Logon to Windows Settings).
Password Policy Monitoring	Do not monitor cardholder password selection. Cardholder password selection will not be governed by a Password Policy. Monitor cardholder password selection according to policy. Cardholder password selection will be governed Password Policy (see below).
Password Policy	Specify required parameters for cardholder Windows password. Windows Password Policy also governs random password generation. With random password generation, the Max. Password Length will specify the password length.
Password Repetition Control	Upon password change allow password repetition. Cardholder password repetition will not be controlled. Upon password change do not allow last password used. Upon password change do not allow last 2 passwords used. Upon password change do not allow last 3 passwords used. Upon password change do not allow last 4 passwords used. Previous passwords will not be allowed as specified.

4.4.5 Website / Application Logon

Parameter	Description
Use Website Logon Auto-Recorder	Checked: Auto-Recorder capability is enabled so Auto-Recorder window is displayed whenever cardholder goes to a website logon location which ConCERTO LOGON recognizes as being recordable. Not checked: Auto-Recorder capability is not enabled. Note: See the Appendix for more information on how the recorder works in relation to websites and applications.
Allow Edit of Website Logon Auto-Recorder	Checked: End-users can change this Auto-Recorder setting (in ConCERTO LOGON Manager General Settings). Not checked: End-users cannot change this Auto-Recorder setting (in ConCERTO LOGON Manager General Settings).
Use Windows Application Auto-Recorder	Checked: Auto-Recorder capability is enabled so Auto-Recorder window is displayed whenever cardholder goes to a Windows application logon location which ConCERTO LOGON recognizes as being recordable. Not checked: Auto-Recorder capability is not enabled. Notes: Administrator can optionally set up a "positive" list which defines for which Windows applications Auto-Recorder will be displayed. See the Appendix for more information. The Appendix also describes how the recorder works in relation to websites and applications.
Allow Edit of Windows Application Auto-Recorder	Checked: End-users can change this Auto-Recorder setting (in ConCERTO LOGON Manager General Settings). Not checked: End-users cannot change this Auto-Recorder setting (in ConCERTO LOGON Manager General Settings).
Max. Number of Fields per Form	Define the maximum number of fields that a logon entry / form entry is allowed to have.
Use Auto-Fill	Checked: Auto-Fill capability is enabled so that when cardholder goes to a logon location which was recorded by the ConCERTO LOGON program ConCERTO LOGON will recognize the location and automatically fill in the logon information. Not checked: Auto-Fill capability is not enabled.
Allow Edit of Auto-Fill	Checked: End-users can change the Auto-Fill setting (in ConCERTO LOGON Manager General Settings). Not checked: End-users cannot change the Auto-Fill setting (in ConCERTO LOGON Manager General Settings).
Submit Option Method	Manually click on submit button to submit logon information. Logon information will be filled in by ConCERTO LOGON, and user clicks on submit button at logon location to submit information. Submit logon information automatically as part of logon process. Logon information will be filled in and submitted as part of the fill process, requiring no additional user intervention
Allow Edit of Submit Option Method	Checked: End-users can change the Submit Method setting (in ConCERTO LOGON Manager Enter Logon Information window). Not checked: End-users cannot change the Submit Method setting (in ConCERTO LOGON Manager Enter Logon Information window).

4.4.6 Website / Application Password Policy

Parameter	Description
Prompt to Change Password Every x Days (0=never)	Define how often cardholder should be prompted to change website/application passwords. Enter number, in days. Number entered in this field will be displayed as default setting in the ConCERTO LOGON Manager software (see ConCERTO LOGON Manager Enter Logon Information window).
Allow Edit of Change Password Prompt	Checked: End-users can change the Change Password Prompt setting (in ConCERTO LOGON Manager Enter Logon Information window). Not checked: End-users cannot change the Change Password Prompt setting (in ConCERTO LOGON Manager Enter Logon Information window).
Use Password Change Verification	Checked: Password Change Verification is enabled so that ConCERTO LOGON will prompt user to verify that password changes they make in the ConCERTO LOGON program have already been made at the logon location. Not checked: Password Change Verification is not enabled.
Allow Edit of Password Change Verification	Checked: End-users can change the Password Change Verification setting (in ConCERTO LOGON Manager Enter Logon Information window). Not checked: End-users cannot change the Change Password Prompt setting (in ConCERTO LOGON Manager Enter Logon Information window).
Password Policy Monitoring	Do not monitor cardholder password selection. Cardholder password selection will not be governed by a Password Policy. Monitor cardholder password selection according to policy. Cardholder password selection will be governed Password Policy (see below).
Password Policy	Specify required parameters for cardholder web/app passwords. Web/App Password Policy also governs random password generation. With random password generation, the Max. Password Length will specify the password length.
Password Repetition Control	Upon password change allow password repetition. Cardholder password repetition will not be controlled. Upon password change do not allow last password used. Upon password change do not allow last 2 passwords used. Upon password change do not allow last 3 passwords used. Upon password change do not allow last 4 passwords used. Previous passwords will not be allowed as specified.

4.4.7 Backup

Parameter	Description
Backup Location	Specify pre-selected path option for location of backup files. Valid options: Default Path Preferred Path This setting will be used when end-users backup the information on their ConCERTO card. Applies also to Auto-Backup default.
Backup Preferred Location	For Preferred location, specify file location.
Allow Edit of Backup Location	Checked: End-users can change the backup location settings (in ConCERTO LOGON Manager Backup / Restore Option). Not checked: End-users cannot change the backup location settings.
Show Print Backup	Checked: End-users will see the "Print Backup" option in the ConCERTO LOGON Manager "Utilities"

Option	menu, which makes it possible for them to print out a hard-copy backup of their logon and personal information. Not checked: End-users will not be offered the "Print Backup" option in the ConCERTO LOGON Manager "Utilities" menu.
Prompt for Auto-Backup	Never prompt for Auto-Backup. Auto-Backup feature will not prompt cardholder to backup data. After data has been saved to card specified number of times. Auto-Backup feature will prompt cardholder to backup data after data has been saved to card specified number of times. Every specified number of days at specified time of day. Auto-Backup feature will prompt cardholder to backup data after lapse of specified number of days at specified time of day.
Specified Number of Times/Days (0 = never)	Define number of times cardholder saved to card, or number of lapsed days, as described above. Number entered in this field will be displayed as default setting in the ConCERTO LOGON Manager software (see ConCERTO LOGON Manager Backup/Restore Utilities).
Specified Time of Day (00:00 - 23:59)	Define time of day Auto-Backup prompt should appear, as described above.
Allow Edit of Auto-Backup Prompt	Checked: End-users can change the Auto-Backup settings (in ConCERTO LOGON Manager Backup / Restore Option). Not checked: End-users cannot change the Auto-Backup settings.

4.4.8 Server

Settings below only refer to smart cards used in "on card" storage mode.

Parameter	Description
Check Server for Hot listed Cards	Checked: Cards issued with this card settings file will check the server for updates. This option must be checked if you are using the "hotlist" card functionality for lost/stolen/returned/defective cards. Note also that for smart cards, when data is stored on the card, you must ensure the "Use Server Functions" under Configuration > Program Settings > Server is also enabled. Not checked: Cards issued with this card settings file will not check the server for updates.

4.4.9 Production

Parameter	Description
Card Operating System Version	Designates the card operating system used, if applicable.

4.4.10 Notes

Parameter	Description
Notes	Free entry field to enter notes relating to card settings files.

4.5 Card Reader Setup

Before you issue cards, you must designate which card reader will be used for Administrator logon and which card reader will be used for end-user card issuance and maintenance ("Production" option).

One reader type may be selected for both functions, or separate readers may be specified.

1. Click on "Configuration" in the menu bar, and click on the "Card Reader Setup" and select "Administrator" or "Production".

2. Card readers which have been installed at the workstation will be displayed in the selection box. Click on selection box to specify the desired reader.

3. Present card to reader, as prompted, to verify card reader setup.

   The card which you present to the reader can be any contact or contactless card from the raw card stock (not yet issued) which is ConCERTO LOGON-compatible. By presenting the card to the reader, the ConCERTO CardMaker verifies that the reader is functional and ready for use for the selected role.

Once readers have been specified, the next time that the Administrator logs on to ConCERTO CardMaker with his card, he will be prompted to use the Administrator reader. Likewise, during card issuance, you will be prompted to present the cardholder card to the Production reader.

As an additional protection for the Administrator card, note that ConCERTO CardMaker will not write anything to the Administrator card which was used to logon to ConCERTO CardMaker in that session - excepting that card PIN changes for that card will still be allowed.

4.6 Using Multiple ConCERTO CardMaker Stations

There are three configuration options for networks that require multiple ConCERTO CardMaker stations:

A	**Independent Mode:**	Independent ConCERTO CardMaker stations use individual program settings and maintain separate databases. Although the ConCERTO CardMaker stations are connected over the network, they do not share information. This is the default mode.
B	**Global Mode:**	ConCERTO CardMaker stations linked over a network that share program settings and a database. To set up: Install ConCERTO CardMaker on each desired machine. Connect each station to the same SQL database. Then confirm that in the ConCERTO CardMaker Configuration menu under Local Settings the setting for "SiteID" is the same for all ConCERTO CardMaker stations. For a description of how to install the SQL database, please ask your reseller for the ConCERTO SQL Server Installation Kit.
C	**Mixed Mode:**	ConCERTO CardMaker stations linked over a network that maintain individual program settings but share a database.

Copyright © 2011 SCM Microsystems GmbH

		To set up: Install ConCERTO CardMaker on each desired machine. Connect each station to the same SQL database. Then in the CardMaker Configuration menu under Local Settings, you must specify the setting for "SiteID" giving each CardMaker station a unique site ID. For a description of how to install the SQL database, please ask your reseller for the ConCERTO SQL Server Installation Kit.

Please refer to the configuration diagrams in the Appendix, for an overview of how each mode works.

5 TOOLS

ConCERTO CardMaker provides the following tools:

- Import data, such as cardholder information.
  (Data export is also described below, although it does not require a ConCERTO CardMaker tool.)
- Compact and repair database, as required.

A description of each tool is provided below.

5.1 Data Import

With the Data Import tool, you can import cardholder information from external data sources, such as Active Directory or a Human Resources database, into the ConCERTO CardMaker cardholder database. The import tool supports ODBC and LDAP according to Microsoft's Active Directory Services Interface (ADSI).

Note also that the "Appendix: Using ConCERTO LOGON with Active Directory", provides additional assistance specifically for administrators who want to synchronize ConCERTO LOGON with Active Directory.

The import function is only available when ConCERTO CardMaker is connected to a data source.

To import data:
Click on "Tools" in the menu bar, and click on the "Data Import" selection. The Data Import window will be displayed.

Data can be imported in two ways:

Import +:
Updates the ConCERTO LOGON cardholder information with new information from the external data source.
- If a matching record is found in the cardholder table, the record fields are updated by the imported data.
- If no matching record is found, a new record is created in the cardholder table.

Import =:
Updates the ConCERTO LOGON cardholder data to match the information from the external data source.
- If a matching record is found in the cardholder table, the record fields are updated by the imported data.
- If no matching record is found, a new record is created in the cardholder table.
- Records in the cardholder table that have no match in the external data source are deleted.

Note when importing data that ConCERTO CardMaker uses the fields "Card ID" and "Cardholder ID" as search index fields. When importing data for cardholders, the field for "Card ID" should not typically be selected for import, since Card ID will be assigned by CardMaker during card issuance. Also before importing, make sure that each cardholder is identified with a unique cardholder ID.
Importing data with ODBC and LDAP are described below.

5.1.1 ODBC

To import data from an ODBC data source:

1. Enter a valid Data Source Name (DSN) in "DSN or Connection String" field. Optionally, you can enter a fully qualified ADO connection string. The following example links to a Microsoft Access database:
   Provider=Microsoft.Jet.OLEDB.4.0;Persist Security Info=False;Data Source=C:\Access.mdb

   The following example shows how to create an ODBC DSN entry in Windows 2000. For more information on ODBC, please consult your Windows operating manual.

   a. Select Start/Programs/Administrative Tools/Computer Management/Data Sources (ODBC).

   b. Select tab System DSN.

c. Click on Add button.

d. Select "MS Access Driver".

e. Enter the name of the DSN.

f. Click on Select… button to select the MS Access database file.

g. Enter user ID and password if necessary (per default, MS Access databases do not require user ID and password).

h. Click on OK to accept the entry and close ODBC. You are now ready to use the DSN by the name you entered in step e. in ConCERTO CardMaker Data Import.

2. Enter user ID and password as required by the data source.

3. Click on Connect button, to connect to the data source. If no error occurs, a list of tables and queries (or "views") will be retrieved from the data source and the status bar will display "Connected to Data Source".

4. The lower frame is now enabled. Click on the pull-down list "Table/Query" to select a table or query (view) from the list.

   You can optionally enter selection criteria to limit the list of records. For example, to limit the list to names that start with "D", enter "LAST_NAME = 'D*'. The selection criteria use SQL syntax of the selected data source. Please consult the respective manual for more information.

5. Click on Select button to retrieve the list of fields for the selected table or query. If no error occurs, the input fields in the right pane will now be enabled.

6. Select fields of the data source and map them to fields in the cardholder table. When a field is selected, the format and size of that field are displayed.

   Optionally, you can enter a conversion format for each entry. See the Appendix for valid format strings.
   Examples: > – convert to uppercase
   < – convert to lowercase
   000-000-0000 – telephone number format
   #.00 – number with two digits past the decimal point

   Click on the Save button to save the data import specifications to file. This is useful in case you need to run recurring updates, for example, on a daily or weekly basis.

7. To retrieve an existing data import specification, click on the Open button and select a data link configuration file.

8. Click on Import + or Import = button to begin the data import process (see description at beginning of this section for more information).

   During the import process, a message is displayed to indicate the activity. When the import is finished, the numbers of records that have been processed are displayed.

5.1.2 LDAP and Active Directory

The CardMaker LDAP interface is based on Microsoft's Active Directory Service Interface (ADSI). See www.microsoft.com/adsi for more information.

This section covers how to generally import user data from an LDAP source. If you want to import user data from

Active Directory and setup your ConCERTO cards to do Windows logon, refer to the Appendix: Using ConCERTO LOGON with Active Directory, which provides an overview of this whole process.

To import data from an LDAP data source:

1. In "DSN or Connection String" field, enter a valid LDAP connection string.

   To connect to the local Active Directory, simply enter LDAP, click on Connect button, and proceed to Step 4.

   Example of an LDAP connection string:
   LDAP://mycomputer:389/CN=Users,DC=mydomain,DC=com

2. Enter user ID ("domain\username") and password. If you connect to the local Active Directory, you can leave these fields blank to use the credentials of the currently logged on user.

3. Click on Connect button to connect to the LDAP server. If no error occurs, the status bar indicates "Connected to LDAP server".

4. The lower frame is now enabled. The pull-down list "Table/Query" displays the AD path to users of the connected Active Directory server. This is for information only.

   You can optionally enter selection criteria to limit the list of records. By default, the list is limited to items with objectClass "user" with an objectCategory of "person", i.e. all users that are persons (and not computers). For example, to limit the list to names that start with "D", add " AND sn = 'D*'" (sn is the surname attribute) to the selection criteria. The selection criteria use SQL syntax. See Microsoft's web site www.microsoft.com/adsi for more information about LDAP-specific limitations.

5. Click on Select button to retrieve the list of mandatory and optional attributes for users. If no error occurs, the input fields in the right pane will now be enabled.

6. Select attributes of the LDAP data source and map them to fields in the cardholder table. LDAP attributes do not support field type and size; these columns remain blank.

   Optionally, you can enter a conversion format for each entry. See the Appendix for valid format strings.
   Examples: > – convert to uppercase
   < – convert to lowercase
   000-000-0000 – telephone number format
   #.00 – number with two digits past the decimal point

   Click on the Save button to save the data import specifications to file. This is useful in case you need to run recurring updates, for example, on a daily or weekly basis. You can also use this file with the Schedule Data Synchronization option, to have data imported on a regular basis.

7. To retrieve an existing data import specification, click on the Open button and select a data link configuration file.

8. Click on Import + or Import = button to begin the data import process (see description at beginning of this section for more information).

   During the import process, a message is displayed to indicate the activity. When the import is finished, the number of records that have been processed are displayed.

5.2 Data Export

External data sources can access the ConCERTO CardMaker cardholder database via ODBC. Consult your Windows operating manual about how to create a System DSN.

5.3 Schedule Data Synchronization

Use this option to schedule the import of user data on a regular basis. You must first have saved a data import specifications file using the Data Import function.

This feature is based on the Windows Task Scheduler, and once the schedule has been saved, it will create tasks that trigger a ConCERTO LOGON data import function. The tasks will be executed as standard Windows tasks within the Windows environment.

To schedule data synchronization:
Click on "Tools" in the menu bar, and click on the "Schedule Data Synchronization" selection. The Data Synchronization Scheduler window will be displayed.

1. Click on the New button, to create a new schedule. You must then select a previously saved data import specifications file (which was saved using the Data Import function) for which you would like to create a schedule.

2. As prompted, enter a task name to help you identify this import task, and save. Note also that the task name will always be preceded by the ConCERTO prefix "ConCERTOCmDataSync" so that it will be recognizable if you access it through the Windows Task Scheduler.

3. Click on the Edit button, to specify the import schedule. Enter your desired parameters into the standard Windows task scheduler tool as required.
   Click on the Delete button, to delete this import schedule.
   Click on the Run Now! Button, to run this import function immediately.
   Click on the Refresh button, to refresh the information displayed on the screen.

Refer to the parameters displayed on the screen for information specific to a selected scheduled task:

Parameter	Description
Program file:	The full path of the ConCERTO LOGON scheduler executable that performs the import task.
Command line:	Includes the full path of the data import specifications file that was saved using the Data Import function and a flag which specifies differential (DIF) or incremental (INC) import. Differential import will be performed as a default, unless you specify INC instead.
Comments:	Add any comments specific to this import function that you want to remember.
Flags:	Any Windows flags that are related to this process.
Last Runtime:	The last time this import procedure was executed by the scheduler.
Next Runtime:	The next time this import procedure will be executed by the scheduler..
Creator:	Identity of person who saved this schedule.
Schedule:	The schedule that was defined, including time of day, frequency, and the date of first execution.
Status:	Current status of this import function.

5.4 Logon Entries Wizard

Administrators can pre-enter logon entries into cards or card accounts, and the ConCERTO LOGON Entries Wizard will prompt the cardholder to personalize the entry with their user name and/or password when they open the ConCERTO LOGON Manager software.

The Logon Entries Wizard will be launched at the start of the ConCERTO LOGON Manager software whenever a logon entry is specified as "... [wizard]". For example, if a logon entry was saved as "GMail [wizard]"in accordance with the description provided below, when the cardholder opens the ConCERTO LOGON Manager software, he will be prompted to enter and

save his GMail user name and password. Thereafter, the entry is ready for use, and the "[wizard]" text will be removed from the entry.

The Wizard functionality is appropriate for use in two cases:

- **Saving Wizard Entries to Cards**
  For installations where the administrator wants to save logon entries to each card before handing them out to end-users.
  See following section for a description of how to save wizard entries to cards.
- **Using Wizard Entries with Managed Entries**
  (For card data that is stored on the ConCERTO CardMaker server.)
  Any installation that uses the standard Managed Entries functionality can include the "... [wizard]" text, to ensure that end-users will be prompted to personalize their logon information. See following sections for a description of how to use wizard entries with managed entries.

Continue on the following pages to see more detailed instructions about saving Wizard entries for Windows logon, and website/ application logon.

When entering Windows logon entries for use with the Wizard, use the following parameters:

* "Use card to logon to Windows..." must be checked in order for the wizard to prompt cardholder to enter Windows logon information.

* Specify a Windows entry name in the following format: ... [wizard], for example Network logon [wizard]

  Note that the entry name (Network logon) must be followed by a space, and then by [wizard] as shown in the following screen shot.

* Wherever you want the end-user to be prompted to enter information, type the text enter here as shown in the screen shot above.

When entering website or application logon entries for use with the Wizard, use the following parameters:

* Use the auto-record functionality, or save entries manually as desired and specify the logon entry name in the following format: ... [wizard], for example Masters online database [wizard]

* Note that the entry name (Masters online database) must be followed by a space, and then by [wizard] as shown in the following screen shot.

* Wherever you want the end-user to be prompted to enter information, type the text enter here as shown in the screen shot above.

5.5 WinLogon Reference Feature

Administrators can use the WinLogon Reference feature to enable website and application logon entries to use the user name and password credentials from a Windows logon entry.

This feature assumes that a Windows user name and password for the cardholder has either already been saved to their ConCERTO LOGON account, or will be saved to their ConCERTO LOGON account upon first use of the software.

When the WinLogon Reference feature is activated for a website or application logon entry, then each time a logon user name or password is required for that logon entry, ConCERTO LOGON will provide the Windows user name and password for logon.

Entries are specified for WinLogon Reference by appending "...[WL:MyWinLogon]" to the entry name. For example, if a

logon entry was saved as "QuickBooks [WL:MyWinLogon]" in accordance with the description provided below, when the cardholder wants to logon to his QuickBooks account, the Windows logon user name and password will be provided.

Note: Be aware that the WinLogon Reference feature is generally best used for logon to websites or applications that are contained within your organization's firewall, so that the Windows logon user name and password are not in use outside of the protection of your network.

The WinLogon Reference feature is appropriate for use in two cases:

- **Saving WinLogon Reference Entries to Cards**
  For installations where the administrator wants to save logon entries to each card before handing them out to end-users.
  See following section for a description of how to save WinLogon Reference entries to cards.
- **Using WinLogon Reference with Managed Entries**
  (For card data that is stored on the ConCERTO CardMaker server.)
  Any installation that uses the standard Managed Entries functionality can include the "…[WL:MyWinLogon]" text, to enable website and application entries to use the Windows logon credentials. See following sections for a description of how to use WinLogon Reference with managed entries.

Continue on the following pages to see more detailed instructions about using the WinLogon Reference feature.

When setting up WinLogon Reference entries, use the following parameters:

* First, as shown in the ConCERTO LOGON Manager screen below, ensure that a Windows logon entry with an Entry Name of "MyWinLogon" has been saved to the user's ConCERTO LOGON account, or that the user will be prompted to save their Windows user name and password to that Entry Name upon first use of ConCERTO LOGON.

  For ConCERTO LOGON versions v.5.0.3+, the default Entry Name of "MyWinLogon" is used for all cards that self-enroll at a ConCERTO LOGON installation.

  Alternately, you may specify another Windows Entry Name, but then you must be sure to use the corresponding name as the WinLogon Reference name instead of "MyWinLogon."

* Next, record the website or application logon entry that you want to have used the Windows credentials, and save the entry to ConCERTO LOGON; or use an entry that has already been recorded. For example, in the sample below, logon to QuickBooks has been recorded.

* In ConCERTO LOGON Manager, select the recorded entry and click on "Change" button to open the entry.

* Append the string "…[WL:MyWinLogon]" to the entry's Name, as shown below.

  Or alternately, if you have chosen to use a different WinLogon Reference name, replace "MyWinLogon" with the Entry Name of the Windows logon entry from which credentials should be accessed.

* As shown below, enter placeholders into the Windows credential fields as follows:

  Into User name field, enter: [WL:USR]
  Into Password field, enter: [WL:PWD]
  Into Domain field, enter: [WL:DMN] (if applicable)

  During auto-fill operations, fields containing "[WL:USR]" will now receive the Windows User Name, fields containing "[WL:PWD]" will receive the Windows Password, and fields containing "[WL:DMN]" will receive the Domain information.

* Save modified entry to card.

Note: If the Windows logon entry specified by "MyWinLogon" cannot be found during auto-fill, only the placeholder values shown above, for example "[WL:USR]", will be filled into the target logon entry.

5.6 Saving Wizard and WinLogon Reference Entries to Cards

(For installations where ConCERTO LOGON data is stored on the card, not on the server.)

Many administrators have a number of standard logon locations that they would like to pre-load to end-user cards. These entries could be Wizard entries, so that cardholders simply need to enter their user name and/or password in order to use the logon entry. Or these entries could be WinLogon Reference entries - entries that use the cardholder's Windows logon user name and password. See previous sections for more information on these two types of entries.

Wizard and WinLogon Reference entries can be saved individually to end-user cards, or this can be accomplished in a more streamlined fashion by saving entries to a ConCERTO LOGON backup file and specifying that the CardMaker software automatically loads the backup file to all end-user cards in a ConCERTO LOGON User Group upon card issuance. Or, the backup file can alternately be loaded to individual cards as desired. The applicable steps are outlined below.

1. **Issue card you will use to store your Wizard and WinLogon Reference entries**
   In the ConCERTO CardMaker software, issue a card that you will use to save the logon entries, calling it for example "Wizard/WinLogonRef entries" card. Refer to "Issue Cards" chapter for additional assistance.

2. **Save Wizard and WinLogon Reference entries to card**
   Open the ConCERTO LOGON Manager software, and use it to record and save Wizard and WinLogon Reference entries to the card, referring to the previous sections for assistance.

   Refer to the "Logon to Windows" and "Logon Entries Screen" chapters in the ConCERTO LOGON Manager User's Manual for additional general assistance.

3. **Create backup file**
   When all desired entries have been saved, use the ConCERTO LOGON Manager Utilities > Backup option to create a backup of the "Wizard/WinLogonRef entries" card.

   If you want to auto-load the Wizard and WinLogon Reference entries to each card in a ConCERTO User Group upon card issuance, you must adhere to the following requirements:

   * The name of the ConCERTO LOGON User Group who should have these entries loaded to their cards must be included in the backup file name in the following format: "PresetEntries_Students.spx"
   In the above example, "Students.ini" is the name of the corresponding ConCERTO User Group. (Note that the ".ini" file ending is not included in the name.)

   * The backup file ("PresetEntries_Students.spx") must be saved or copied to the ConCERTO CardMaker server under "Program Files\ConCERTO CardMaker\Data".

   * You must specify the backup password as "12345".

   If you want to load the backup file to individual cards:
   You can specify any backup file name and any backup password, and save the backup file to any desired location.

4. **Load backup file to end-user cards**

   If you followed the instructions above to auto-load the Wizard and WinLogon Reference entries to each card in a ConCERTO LOGON User Group upon card issuance:
   Simply issue smart cards as usual and the entries will be automatically loaded to the cards of all members of the

specified ConCERTO LOGON User Group upon card issuance.

If you opted to load the backup file to individual cards:
Issue cards as usual. Then, after you have issued the end-user cards, open the ConCERTO LOGON Manager software and "restore" the backup to each end-user card, referring to the "Backup/Restore" chapter in the ConCERTO LOGON Manager User's Manual for additional assistance. Note that you will need to open and close the Logon Manager application for each new card.

If you would like to further personalize logon entries for individual cardholders, after loading the backup to each card, you can edit the entry information further if desired. For example, if you want to pre-enter user names into the Windows logon entry, this would be the time to do it. Then as before, for each entry data field that still contains the text "enter here", the cardholder will be prompted to enter their personal logon data.

5.7 Using Wizard and WinLogon Reference Entries with Managed Entries

Any installation that uses the standard Managed Entries functionality can use Wizard and WinLogon Reference Entries with managed entries.

Wizard and WinLogon Reference entries are entered into the managed entries template card in the standard fashion. Refer to "Managed Entries" chapter that follows for additional assistance with managed entries.

5.8 Managed Entries

With the ConCERTO CardMaker software, the Administrator does not need to create software links - via scripts and agents - to the applications for which he wants to create managed entries, as with many single sign-on systems.

Instead, the Administrator simply creates a logon entry using the ConCERTO LOGON Manager interface and saves it to an ID card from the card stock which he will be using. When the administrator "auto-records" the logon entry, ConCERTO "learns" the logon location of the entry, and the entry format for the user name and password.

The ID card which the Administrator uses to create managed logon entries is then referred to as the "managed entries template card", since the Administrator can save the formats for multiple managed entries using this template card. He then uses the logon information from this template card to load the managed entries to the cards or ConCERTO accounts of user groups or individual end-users. The complete process is described in more detail below.

Note also that the "Appendix: Using ConCERTO LOGON with Active Directory", provides additional assistance specifically for administrators who want to manage Windows logon entries.

5.8.1 Managed Entries Preparation

Prepare for managed entries creation as follows:

1. **Ensure that ConCERTO LOGON Manager Software is installed on administrator computer**
   The "Create Managed Entries" function uses the ConCERTO LOGON Manager software interface, so the ConCERTO LOGON Manager software must also be installed on the administrator computer.

   Be sure to also select the correct card and reader from Start > Programs > ConCERTO LOGON Manager > Card and Reader Configuration, before starting the program.

2. **Ensure that the "Modify access permissions" step has been performed**
   You will find this step in the "Installation" section of this manual. The server functionality will not be able to function correctly unless this step has been completed.

3. **Create a "User Group Card Settings file" for the managed entries template card**
   You must create a user group card settings file under Configuration > Card Settings that will have the same name as the template card, since this is how the template card will be assigned to end-users when they are issued cards or when they self-enroll.

In other words, when an end-user self-enrolls or is issued a card, depending on which User Group they are assigned:
- End-user card will be assigned the card settings for that user group.
- End-user card will be assigned the managed entries for that user group (if a managed entries template card has been created for that user group).

Go to Configuration > Card Settings to save a user group card settings file, for example, save a user group card settings file for the "Manager" user group as follows:
Card Settings file: "Manager.ini"

When you issue your managed entries template card in the next section, you must then specify the cardholder ID beginning with "Template..." followed by the user group name, for example, for the "Manager" user group:
Matching managed entries template cardholder ID: "TemplateManager"

5.8.2 Create Managed Entries

Create managed entries using a "managed entries template card" as described below.

1. Take an ID card from card stock, which will be used as a managed entries template card. Using ConCERTO CardMaker, click on "Card" then "Issue Card" to create a cardholder account with a Cardholder ID that starts with "Template..." followed by the name of the user group for this template card (see "User Group Card Settings file" specifications above). This enables the ConCERTO LOGON system to recognize this card as a template card, and enables it to be assigned to all end-users who are assigned to this user group.

   For example, for the "Manager" user group, the fields must be specified as follows:
   Cardholder ID: TemplateManager
   User group: Manager.ini (created previously in Configuration > Card Settings)

   You can then specify the other data as desired, for example:
   Last name: Template
   First name: Manager
   Department: Templates

2. After the card has been successfully issued, click on "Tools" and click on "Create Managed Entries" option. This will open the ConCERTO LOGON Manager software interface. Note that the "Cardholder ID" of the card that you use with this interface must begin with "Template..." in order for card to be recognized within the CardMaker system as a template card.

   Create Windows, website and application logon entries in the ConCERTO LOGON Manager interface, to be used as managed entries, and save them to the template card's ConCERTO LOGON account.

   Tips:
   * Template entries can be created with user name and password, or user name and password can be left blank, to be specified individually later using the "Assign Managed Entries" function.

   * The most important thing about creating the template is "teaching" ConCERTO LOGON how to get to the logon location and enter the logon credentials. This can be done using either ConCERTO LOGON' auto-record feature, or by clicking on the "New" button in Logon Manager and creating a new entry manually.

   * If you want the Logon Entries Wizard to prompt cardholders to enter their user name and/or password for a logon entry, append the text "[wizard]" to the end of the logon entry name and type the text "enter here" into each entry data field that you want the cardholder to personalize. Refer to the „Logon Entries Wizard" chapter for additional assistance.

   * If you want the entry to use the cardholder's Windows logon user name and password as the logon credentials for the entry, use the WinLogon Reference feature, as described in the preceding section.

   * Any other settings that you change on the template card will be transferred to end-users cards that are issued or that self-enroll for this user group. If preferred, do not change any settings directly on the template card - instead, change

card settings as desired directly in the Configuration > Card Settings file for this user group. This will ensure that the user group card settings match the template card for this user group at all times (see also below).

* Once cards are in the field: if you update managed entries on the template card, note that only the managed entries themselves and the "Permissions" associated with the managed entries can subsequently be updated to end-user cards in the "Assign Managed Entries" screen. To update user group card settings in the field, you must go to Configuration > Card Settings, change card settings for the user group as desired, and save your changes. You will then be prompted if you want to update these card settings to the template card (for cards that will be subsequently issued), and to cards already in the field.

* You must use the "Create Managed Entries" selection from ConCERTO CardMaker to open the Logon Manager interface when you create managed entries. Entries created in a normal Logon Manager interface will not be recognized as managed entries.

5.8.3 Assign Managed Entries with Card Issuance

Managed entries will be loaded to the card accounts of all end-users who are assigned to the corresponding user group before they self-enroll or are issued a card from ConCERTO CardMaker.

End-users who self-enroll will be recognized within the system by the "Cardholder ID" field, which must be a unique number, or the "Windows/ConCERTO User Name" field, or both. Most installations use an already existing "Employee/Student ID" number, which the employee already knows, or, if end-users know their Windows user name, this is also appropriate.

If no user group is assigned to an end-user before card issuance, the end-user will be automatically assigned the "Default User Group Card Settings file", which you can specify in Configuration > Program Settings.

1. To assign an end-user to a user group, click on "Card" and click on "View/Edit Cardholder" option.

   If you previously imported your HR database into CardMaker…
   Assign individuals to the correct "User Group" as required. Or, if your HR database is large, you may want to consider importing that database in a way that already assigns the user group in accordance with classifications already specified in the original HR database.

   To enter individuals manually…
   Enter cardholder data as described in the "Card Issuance" section and assign "User Group" as required.

2. Issues cards as manually as described in „Card Issuance"section or allow end-users to self-enroll.

   If end-users will be self-enrolling, be sure that the "Cardholder ID" specified matches the "Employee ID" that they will enter upon self-enrollment, or make sure that end-users know their Windows User Name, to ensure that they are assigned to the correct user group and receive the correct card settings and managed entries.

5.8.4 Assign Managed Entries to Cards Which Were Entered or Issued

Managed entries can be assigned to a user group or individual for cards which have already been entered into the system, or are already in circulation, as described below.

1. Click on "Tools" and click on "Assign Managed Entries" option.

2. Select template card: click on the template card that you want to assign managed entries from, on left side of screen.

3. Click on "Copy to" button to copy managed entry to a different user group or an individual cardholder. Select user group and cardholder on right side of screen to copy entry to. Click on "Paste" button to paste entry. Click on "Clear" button in upper left corner to clear paste function.

   Click on "Change" button to change a managed entry on a managed entries template card. Note that only logon credentials can be changed here. If you want to change the way a logon functions, you must change this in the template card directly using the Logon Manager interface via "Create Managed Entries" option. Administrator can also specify if

the end-user will be allowed to view, edit all, edit password, or delete the managed entry.

Click on "Delete" button to delete a managed entry on a managed entries template card.

4. To change logon credentials for a user group or cardholder: Select user group, cardholder, and managed entry on right side of screen. Click on "Change" button and change logon credentials as desired. Administrator can also specify if the end-user will be allowed to view, edit all, edit password, or delete the managed entry. Note also that Administrator may never view a password, but can reset a password.

5. To delete managed entry for a user group or cardholder: Select user group, cardholder, and managed entry on right side of screen. Click on "Delete" button to delete entry.

5.8.5 Set Windows credentials

In the Assign Managed Entries screen, click on the Credentials button, then click on an individual cardholder or the Select All button, to set the Windows logon credentials for and individual or a group.

Click on the Set Credentials button, and choose the options that best suit your installation. Refer to the table below for assistance.

Set user name of selected Windows logon entry to value of 'CardholderID'.	**Recommendation:** If you imported end-users from Active Directory, this option can always be selected. **Why:** During import, the 'CardholderID' field in CardMaker is filled from the Windows logon User Name field in Active Directory.
Set to default password. Default password = …	**Recommendation:** Select if you want to specify a default password, for example, if you want to specify a default password for new users that they are required to immediately change. **Why:** Default passwords can be helpful for individuals as well as groups, depending on your needs.
Set to random password.	**Recommendation:** Select if you want ConCERTO LOGON to create a random password for each individual end-user that was selected on the previous screen. **Why:** This option is appropriate for two scenarios: if you will be completely managing the Windows passwords and the end-user will never know his Windows password. Or, if you want to provide each end-user with their Windows password, you can print out a Password Letter for each individual end-user (under Reports).
Do not change password.	**Recommendation:** Select if do not want ConCERTO LOGON to change the Windows password for the selected end-users. **Why:** Selecting this option will not affect the password entry in Active Directory if you have elected to synchronize Windows password changes with Active directory, and will leave the Windows logon password field for each end-user card account blank. This is appropriate, for example, if end-users will be specifying their own Windows logon passwords.

Click on Set Credentials button, to set end-user credentials as specified.

Important Note: If you want a Windows password change to be also immediately synchronized with Active Directory, you must have the "Synchronize Win Password Changes with Directory" option checked under Configuration > Program Settings > LDAP/Active Directory. Otherwise, Windows password changes will never be synched with Active Directory, and you will have to enter changed passwords into Active Directory manually.

5.8.6 Assign Bulk Managed Entries to Cards by Exporting to Excel File

Instead of assigning user names and passwords individually, you can also assign them in bulk by exporting a credential

file to Excel, entering the credentials in bulk, then importing the file back into ConCERTO CardMaker.

To export a managed entries credential file:

1. Click on "Tools" then click on "Assign Managed Entries" option, and click on the "Export" button. A message box will describe that the Export function will create a "TAB-delimited" .txt file that can be opened in Excel. Click on the "OK" button to continue.
2. Select a user group and/or cardholder, then highlight the managed entries that you want to export, by holding down the "Shift" button, or by clicking on the "select all" button. Click on the "Export Credentials" button to continue.

3. Specify a .txt file name and location, as prompted by the next window, then click on "Export Credentials" button to complete export function.

To assign credentials in Excel file after successful export to .txt file:

1. Open Excel software, and open .txt file specified above using the standard Excel "File > Open" selection.

2. Use the standard default settings offered by Excel "Text Import Wizard" for "Delimited data" by clicking the "Next" button through the wizard screens.

3. Adjust columns to desired width, change individual credentials as required, and save .txt file when complete.

To import .txt credential file back into ConCERTO CardMaker:

Click on "Tools" then click on "Assign Managed Entries" option, and click on the "Import" button. Select the .txt credential file specified above, and click on the "Import Credentials" button to complete import.

5.9 Compact/Repair Database

To compact/repair database:

Click on "Tools" in the menu bar, and click on the "Compact/Repair Database" selection. This procedure may include options which are specific to your installed database (consult your system Administrator).

6 SYSTEM MAINTENANCE

6.1 Re-issue Card

An Administrator may need to re-issue ConCERTO cards to cardholders, when a card is lost, stolen or defective.

- Cards can be re-issued to existing cardholders, which are listed in the system's cardholder database.
- Before re-issuing a card to an existing cardholder, the old card of the cardholder must be reported as lost, stolen, defective, or returned (one card per cardholder policy). See following section, to report card as lost, stolen, defective, or returned.
- If card is an Administrator card, note that Administrator rights must be activated again under "Configuration" then "View/Edit Administrator Rights" so that a check appears in the checkbox next to "Active".
- Cardholder can save the card backup file which was created with their previous card to their new card, as long as they remember the backup password that they used.
- Card users in server mode who are allowed to "self re-enroll" can load their data to a new card from the server, even if they did not make a backup - as long as they know their ConCERTO LOGON User Name and PIN.
- When the Administrator personally re-issues a card to a server mode card user, the cardholder will be able to access his previous data file using his card PIN from the previous card.

IMPORTANT: Before you re-issue a card, it is necessary to obtain positive proof of the cardholder's ID, to ensure the security of the system.

To re-issue ConCERTO cards:

1. Click on "Card" in the menu bar, and click on the "Issue Card" selection.

2. Click on the box on the left side of the cardholder's entry that you want to select, and click on the Select button. ConCERTO CardMaker will automatically proceed in the re-issuance mode when the selected card has a lost, stolen, defective, or returned status.

3. CardMaker will prompt you to present a new ConCERTO card to the card reader. Card will be processed, and the system will prompt you when you may remove the card and deliver it to the cardholder.

   Note: You should inform the cardholder that he can now load any backup files which were created with his old card, to the new card. Cardholder must know the backup password he specified when he created his backup, in order to load the previous backup to the new card.

6.2 Self Re-enroll

Card installations which allow "Self Enrollment" can also allow end-users to "Self Re-enroll" if they lose their card and are given a new ID card.

The "Self re-enrollment only allowed for hot-listed cards" option under Configuration > Program Settings > Server enables you to only allow self re-enrollment for cardholders that are entered on the hotlist. Cards can be added to the hotlist for lost (stolen, defective, returned) cards under Card > Add Card to Hotlist.

Self Re-enrollment proceeds as described in the "Self Enrollment" section of this manual, except that end-user must be sure to correctly enter their employee ID and the same ConCERTO User Name into the registration form that they entered originally if they want to access their previous data. Once the system recognizes the cardholder, it will prompt the cardholder to enter the card PIN of his previous card in order to access the previous data. Thereafter, that data will be associated with the end-user's new card.

Copyright © 2011 SCM Microsystems GmbH

6.3 Report Lost/Stolen/Defective/Returned Card

Use this section to report a lost/stolen/defective/returned ConCERTO card to the CardMaker system. After entering this information, you can then re-issue a ConCERTO card to the cardholder, using the Re-issue Card instructions, above.

By declaring a card lost, stolen, defective, or returned, the card will be hot-listed. If the installation is set to block the use of hot-listed cards within the system (see "Check Server Hotlist" option under Card Settings), this will inhibit the card from being accepted for logon actions with ConCERTO LOGON Manager and will lock hot-listed smart cards when ConCERTO detects that they have been inserted into a card reader. Cards which have been "hot-list locked" cannot be unlocked.

To report a lost/stolen/defective/returned card:

1. Click on "Card" in the menu bar, and click on the "Add Card to Hotlist" then the "Report Lost/Stolen/Defective/Returned Card" selection.

2. Select the lost/stolen/defective/returned card from the issued cards list and click on the "Select" key.

6.4 Identify Card

To identify a card, for example, if there is no name or photo on the card:

1. Insert card in card reader.

2. Click on "Card" in the menu bar, and click on the "Identify Card" selection. If the card has been issued, the cardholder's information will be displayed.

6.5 Update Card Settings

To update card settings on a card without affecting any of the data that is stored on the card:

1. Present card to card reader.

2. Click on "Card" in the menu bar, and click on the "Update Card Settings" selection. The card settings will be updated to the new card settings that have been defined for that card.

Updates to contact chip cards must always be performed with Administrator assistance, as described above, unless the contact chip card is used in server mode.

For RFID cards, card settings can also be updated at any time for an entire user group card settings file by updating the card settings as desired under Configuration > Card Settings. When the updated card settings file is saved, ConCERTO will offer to automatically update the card settings of all cards in the field with that user group card settings file.

However, whenever the card settings update involves changing the user group card settings file name for a particular cardholder, it must be Administrator assisted, as described above.

6.6 Change PIN

Cards which are issued to end-users have no special rights at the time of issuance, so it is not necessary to change the PIN on the card until the individual user has saved personal information to the card. Cardholders who use the default PIN of "12345" are prompted to change their PIN in the ConCERTO LOGON Manager software the first time that they use the system.

Copyright © 2011 SCM Microsystems GmbH

If you are assigning Administrator rights to a ConCERTO card, the card PIN should be changed immediately, so that the Administrator rights are protected.

To change your card PIN:

1. Click on "Card" in the menu bar, and click on the "Change PIN" selection.

2. Type in the current card PIN (manufacturer's default is "12345").

3. Choose a new PIN, and enter it twice, as shown.

   Note: If you choose to write your card PIN down, you must store this information in a secure place, so that the security of your ConCERTO card is not compromised.

4. Click on the OK button.

6.7 Reset Card PIN

Organizations that are running in server mode and require the reset card PIN feature can ask their reseller to enable this feature for them. By default, this feature is typically not activated.

Card PIN and PUK will be reset to the ConCERTO default "12345", unless the PUK was specified as admin-managed. If you originally specified an admin-managed PUK, the PUK will remain the same, but the PUK counter will be reset, in case the wrong PUK was already entered repeatedly.

Note also that the administrator can reset the PIN without requiring the presence of the card. Administrator would then inform cardholder that his PIN has been reset to "12345" and that cardholder should change the PIN upon first use.

To reset a card PIN:

1. Click on "Card" in the menu bar, and click on the "Reset PIN" selection.

2. A list of all cards running under server mode will be displayed. Click on desired card, then on Select button. Confirm PIN reset, as prompted.

6.8 View/Email User PIN/PUK

Under Configuration > Card Settings > PIN > PIN/PUK Assignment Method, if you selected "Generate random PIN and random PUK", this PIN/PUK pair can be viewed or emailed using this feature. This feature would typically be used if the management of the PIN/PUK will be completely in the hands of the cardholder.

Be aware that with this selection, the PIN/PUK can be changed by the cardholder, so this PIN/PUK pair may not be usable if the administrator wants to be able to unlock an end-user's card with the PUK.

To view/email the user PIN/PUK:

1. Click on Card > View/Email User PIN/PUK. Use "Find" button to select cardholder name or ID# from list.

2. Click on "Select" button to view PIN/PUK, then click on Email button, to email information to cardholder, if desired.

Note that emails will be sent automatically only when the cardholder's email address was entered into the cardholder record in the email field. Note also that the email server settings must be configured for your installation under Card > View/Email User PIN/PUK. Click on the Email button and enter the access information for your SMTP server.

Alternately, administrators can print out the PIN/PUK letter under Reports > PIN Letter and distribute it to the cardholder as desired.

Copyright © 2011 SCM Microsystems GmbH

6.9 View/Email Admin PIN/PUK

Under Configuration > Card Settings > PIN > PIN/PUK Assignment Method, if you selected "Use default PIN (12345) and admin-managed random PUK", this PIN/PUK pair can be viewed or emailed using this feature. This feature would typically be used if the administrator wants to control the use of the PUK in order to be able to unlock end-user cards.

To view/email the admin PIN/PUK:

1. First, confirm the ID of the cardholder before providing the card PUK.

2. Click on Card > View/Email User PIN/PUK. Use "Find" button to select cardholder name or ID# from list.

3. Click on "Select" button to view PIN/PUK, then click on Email button, to email information to cardholder, if desired. Or if desired, have cardholder present their card, enter PUK to unlock card, and ask the cardholder to specify a new PIN.

Administrators can choose to setup the email server settings so that a PIN/PUK letter is emailed out to each new cardholder, so that cardholders also have their card PUK available in case they lock their cards. Or, administrators can email the PUK to the cardholder as required. Alternately, administrators can print out the PIN/PUK letter under Reports > PIN Letter and distribute it to the cardholder as desired.

Note that emails will be sent automatically only when the cardholder's email address was entered into the cardholder record in the email field. Note also that the email server settings must be configured for your installation under Card > View/Email Admin PIN/PUK. Click on the Email button and enter the access information for your SMTP server.

Another option: If there are multiple computer centers and you want trusted administrators at each center to be able to unlock cards, it is also possible to save the Admin PUK information to a drive letter on a secure server so that is accessible by all trusted administrators. To map Admin PUK information to a drive letter on a secure server, proceed as follows:

a) Using Windows Explorer, go to "Program Files\Power LogOn Admin\" and locate the "PukLetter (admin)" folder.
b) Map the whole "PukLetter (admin)" folder to the drive letter on a secure server, **being sure to make the folder "Read only"**.

Inform trusted administrators of the location of the "PukLetter (admin)" folder. The PUK for individual cardholders can be located using the Cardholder ID (student ID).

7 Backing Up, Restoring, and Updating System

ConCERTO CardMaker stores configuration and card-related data. In order to ensure that you can fully recover the system in case of a crash or a release update that requires uninstalling the previous version, it is mandatory to perfom scheduled backups.

7.1 Backup All CardMaker Data

For a full backup of ConCERTO CardMaker data, at least the following configuration and cardholder-related files must be backed up as described below.

1. Backup Configuration Files
   'C:\Program Files\ConCERTO CardMaker\CardMaker.ini'
   'C:\ Program Files \ConCERTO CardMaker\rfip.ini'
   'C:\ Program Files \ConCERTO CardMaker\CardSettings*.*'

2. Backup Server-based Card Data
   'C:\Program Files\ConCERTO CardMaker\Data*.*'

3. If you are using CardMaker with MS SQL database, you must also backup the SQL files:
   ConCERTO_cardholder.mdf
   ConCERTO_txlog.mdf
   (the above 2 files are located in the MS SQL data directory - i.e. "C:\Program Files\Microsoft SQL Server\MSSQL\Data\")

7.2 Backup Cardholder Data Only

If you only want to backup cardholder data, proceed as described below.

1. First, make sure that the CardMaker program is closed. Then, open Windows Explorer and go to the file area C:\Program Files\ConCERTO CardMaker\Data

2. Right-click on the "Cardholder.mdb" file and click on the "Rename" option. Change the name of this file to another name, for example, "DamagedCardholder.mdb".

3. Right-click on the "Cardholder.bak" file and click on the "Rename" option. Change the name of this file to "Cardholder.mdb". CardMaker will now use this file as the database.

7.3 Restore ConCERTO CardMaker Data

In case of a system crash, re-installation of CardMaker or porting of the CardMaker software to another server computer, it may become necessary to restore previously saved backup files as described below.

1. If installation is on a Terminal Server, logon in console mode, and make sure that there are no other Terminal Services sessions open.

2. Exit all CardMaker and ConCERTO LOGON applications.

3. Restart IIS.

4. If all previous data as well as card and program settings are to be restored, copy the backup files listed above under "Backup All CardMaker Data" into their original folder locations.

Notes:
* Make sure that the CardMaker version that you are updating to supports the same configuration file and database

structure of your previous version. Consult any documentation that comes with the update and/or consult with your ConCERTO distributor or ConCERTO manufacturer.
* Also, if you restore a previous backup to a different server computer, remember that you must get a new rfip.ini file from the distributor/manufacturer, to match the new server computer's IP address. Then you must copy this new new rfip.ini file to all of your client computers that run the ConCERTO LOGON Manager program. See Server Setup section in the Getting Started chapter of this manual for additional information.

7.4 Un-installing and Re-installing/Updating ConCERTO CardMaker

1. If installation is on a Terminal Server, logon in console mode, and make sure that there are no other Terminal Services sessions open.

2. Exit all CardMaker and ConCERTO apps (if running).

3. If there is a previous installation, make a backup copy of for all configuration and server-based card data (see backup instructions above).

4. Restart IIS.

5. From Desktop > Start > Control Panel select Add/Remove Programs.

6. Select "ConCERTO CardMaker" and click on the "Change/Remove" button. Follow on screen instructions to completely un-install.

7. Delete the directory tree "C:\Program Files\ConCERTO CardMaker" with all remaining files.

8. Install updated version of ConCERTO CardMaker. Follow installation and configuration instructions in the CardMaker User's Manual.

9. Optionally restore any previously backed-up configuration and card data as outlined under "Restore CardMaker Data" above.

Or, if the database of the new CardMaker installation is not compatible with the previous one, use the CardMaker import function as described in this manual.

7.5 Un-installing and Re-installing/Updating ConCERTO LOGON Manager Software

1. If installation is on a Terminal Server, logon in console mode and make sure that there are no other Terminal Services sessions open.

2. Ensure that in ConCERTO LOGON Manager, the checkbox "Settings > Logon to Windows > Use card to logon to Windows .." is unchecked.
   - If already unchecked, then proceed with step 2.
   - If checked, then uncheck and save settings to card and reboot.

   Note: If for some reason you are unable to open ConCERTO LOGON Manager you can also manually deactivate the ConCERTO GINA by deleting the following string value in the Windows Registry:
   "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\GinaDLL".
   Before deleting this value, ensure that it was set to "odgina.dll". If it is pointing to any other component, it was not created by ConCERTO.

3. From Desktop > Start > Control Panel select Add/Remove Programs.

4. Select "ConCERTO LOGON Manager" and click on the "Remove" button. Follow on screen instructions to completely un-install.

5. Install new version using the Installation Options menu on the ConCERTO Setup CD.

6. After re-installation of the ConCERTO LOGON Manager software, you must make sure that the rfip.ini file still matches the CardMaker rfip.ini file on the server that the client should connect to. See Server Setup section in the Getting Started chapter of this manual for additional information.

7. Remove card from reader.

8. Start the ConCERTO Card and Reader Configuration wizard, select the matching card / reader pairing and click OK.

9. At the "Insert card" prompt, select the desired operating mode (Server/Standanlone/Demo ...), and insert card.

Copyright © 2011 SCM Microsystems GmbH

8 REPORTS

8.1 Cardholders

To view a report of all cardholders those have been entered into the system:

1. Click on "Reports" in the menu bar, and click on the "Cardholders" selection then "All", "Users" or "Administrators". For this report, you can also further specify between Active and Inactive cardholders.

2. Click on the Preview button, to view a formatted report on your screen.

3. Click on the Print button, if you want to send a report to a printer.

8.2 Pre-entered Cardholders

To view a report of all cardholders those have been pre-entered into the system but have not yet been issued cards:

1. Click on "Reports" in the menu bar, and click on the "Pre-entered Cardholders" selection.

2. Click on the Preview button, to view a formatted report on your screen.

3. Click on the Print button, if you want to send a report to a printer.

8.3 PIN Letter

To print a PIN letter for a cardholder, after the cardholder has been issued a ConCERTO card:

1. Click on "Reports" in the menu bar, and click on the "PIN Letter" selection.

2. PIN letter file names include the "Cardholder ID number", followed by the "Last Name" followed by the "Date Issued". Click on the PIN letter file you want to print, and click on the Open button.

3. To print the PIN letter, click on "File", then the "Print" selection.

Note for SafeSign CSP option users: Since all PIN information is regulated by the SafeSign software, you will not be offered the PIN Letter option in ConCERTO.

For installations which use a PUK, the PUK will also be included in the PIN letter.

8.4 Password Letter

To print a Password letter for a cardholder, after the cardholder has been issued a random Windows password (under Assign Managed Entries > Credentials):

1. Click on "Reports" in the menu bar, and click on the "Password Letter" selection.

2. Password letter file names are listed on a screen that is similar to the PIN letter screen as shown above, but are preceded by "WLC" for Windows logon credential, followed by the "ConCERTOUserName". Click on the password letter file you want to print, and click on the Open button.

3. To print the Password letter, click on "File", then the "Print" selection.

Copyright © 2011 SCM Microsystems GmbH

8.5 Hot-listed Cards

To view a report of all hot-listed cards - cards that have been reported to the system as having been lost, stolen, defective or returned:

1. Click on "Reports" in the menu bar, and click on the "Hot-listed Cards" selection then "All", "Lost", "Stolen", "Defective" or "Returned".

2. Click on the Preview button, to view a formatted report on your screen.

3. Click on the Print button, if you want to send a report to a printer.

8.6 Card Inventory

To view the card inventory report:

Click on "Reports" in the menu bar, and click on the "Card Inventory" selection.

8.7 Transactions

To view the transaction report, this includes logon and logoff to Windows of individual cards if you are using the server option.

Click on "Reports" in the menu bar, and click on the "Transactions" selection, then "All" or "Selected Cards".

Copyright © 2011 SCM Microsystems GmbH

9 Support

You can use the support links to go online to the administrator support site and view documentation, a ConCERTO LOGON Enterprise Tutorial, and FAQs. When you click to the support site from the ConCERTO CardMaker software, no user name and password is required.

The administrator support site is also available from the ConCERTO website at http://support.scmmicro.com/ConCERTO.

10 Appendix: Using ConCERTO LOGON with Active Directory

This section provides a step-by-step overview of how to import end-users from Active Directory, and transition them from manual Windows logon to card-enabled Windows logon.

The first section describes an "automated" option, where you setup ConCERTO LOGON for self-enrollment and schedule synchronization with Active Directory, and then just let the system run. The second section describes a more "managed" option, where you can have more choices about how you want to handle the system.

The final section describes a feature that is especially useful for organizations that frequently have new users, such as schools. When you switch this feature on, instead of having to enter new users into Active Directory, ConCERTO LOGON will create a new Active Directory account for new end-users upon card issuance. ConCERTO LOGON also updates the Active Directory accounts of existing users, so that all cards are ready to be used for logon within the network.

10.1 Setup to run automated: for users known to Active Directory

This section describes an "automated" option, where you setup ConCERTO for self-enrollment and schedule synchronization with Active Directory, and then just let the system run.

The setup method described below is the easiest way to get users migrated from manual to card-based logon. Assuming that end-users are already known by Active Directory, this method will synchronize user data with Active Directory and allow users to self-enroll using their current user name and password. Users that are added to Active Directory are automatically able to self-enroll, while users that are deleted from Active Directory are also deleted from ConCERTO LOGON. Subsequent to self-enrollment, the password can be changed by the administrator and can be kept invisible to the end-user.

Administrator proceeds with the following steps in ConCERTO CardMaker:

1. Specify desired card settings for default user group
2. Import end-user data from Active Directory
3. Issue template card for default user group
4. Save a "Default" Windows logon entry on template card
5. Configure self-enrollment options
6. Change Windows passwords for all cardholders

Each step is explained in more detail below. You may also refer to the individual section in this manual for additional information on any of the above topics.

1. Specify desired card settings for default user group

You must first specify the card settings that you want to use as a default, so that the end-users that are imported from Active Directory will automatically be assigned to the default user group. If you have a large number of individuals who will be assigned the same card settings, it is recommended that you use this user group as your default user group - by naming this group for example, "GeneralUser".

> TIP: You can always create a more exclusive user group with different card settings, to be assigned to management personnel, for example. In this case, you would then change the User Group specification of the management individuals after import from Active Directory has been completed, under Card > View/Edit Cardholder.

Continuing for this example with the "GeneralUser" user group, go to Configuration > Card Settings. Specify card settings as desired and save as "GeneralUser". When prompted if you want to designate file "GeneralUser.ini" as the Default User Group Card Settings File", click on Yes.

2. Import end-user data from Active Directory

1. Go to Tools > Data Import > Open. Click on the sample file which has been provided, as a template. You will get an error message, since the sample file does not yet contain information which is specific to your installation.
2. Change the DSN or Connection String to your access parameters. In many cases, you just need to change computer name, and domain. Note that a DNS recognizable name is preferable to IP address if you are using SSL.
3. Enter the administrator login User ID and Password that give you privileges to access Active Directory.
4. Click on Connect. After successful connection, click on Select.
5. You may now specify the Field Names that you want to import. If you import the field names as depicted in the image above and specified below, this will be sufficient to ensure a good working relationship between Active Directory and CardMaker:
   Card_ID: (leave blank)
   Cardholder_ID: (leave blank)
   ConCERTOUserName: userPrincipalName (ie, sbeaton@mydomain.com)
   Last_Name: sn
   First_Name: givenName
6. Click on the Save As button to save the data import specifications to file. Save the file with a easily recognizable name, and you can then use this file to execute future imports, or with the Schedule Data Synchronization option, to have data imported on a regular basis.
7. Click on "Import=" if you want to ensure that only end-users who are listed in Active Directory will be listed in CardMaker. Or, click on "Import+" if you want to only add new end-user information to the CardMaker list. See the Data Import section, for additional information.
8. To view the end-users who have been imported into CardMaker, go to Card > View/Edit Cardholder:

In order to periodically run an import task against Active Directory, you can specify a new task under Tools > Schedule Data Synchronization. See also the Schedule Data Synchronization section in this manual.

3. Issue template card for default user group

You will now create a template card which will enable you to transfer a Windows logon entry to all cardholders in a user group.

1. Go to Card > Issue Card > Add New. Take a card from the card stock and present it to the reader.
2. Ensure that the default user group for the template card is the previously created default card settings file, in the case of our example, "GeneralUser". Then specify the Cardholder ID for the template card as "TemplateGeneralUser", for example.
3. Click on Issue button to issue the template card.

4. Save a "Default" Windows logon entry on template card

1. Go to Tools > Create Managed Entries. The Logon Manager application will open.
2. Using your template card, create a Windows logon entry under Settings > Logon to Windows, and fill out its fields as follows:
   Entry Name: "Default Logon"
   The value "Default Logon" in this field ensures that this Windows logon entry will be automatically designated as the default Windows logon entry in end-user card accounts during self enrollment.
   User name: "Default Logon"
   The value "Default Logon" will be replaced with the cardholder's Windows user name during self enrollment. The Windows user name is expected to be stored in the cardholder field "ConCERTOUserName", where it was placed during step 2 "Import end-user data from Active Directory". Note that the field "ConCERTOUserName" must hold the full windows user account name (for example "myuser@mydomain.com").
   Password: Any value.
   Depending on the self enrollment program settings, the password field will be filled with a value entered by the user. Otherwise, if the user will not be prompted to enter a password, the password can be preset individually or with the "Credentials" function under Tools > Assign Managed Entries.

Domain: "Default Logon"
The value "Default Logon" will be replaced with the cardholder's Windows domain name.

3. Change Permissions as desired, and save.
4. Close Logon Manager application.

5. Configure self enrollment options

The options selected in the Program Settings screen shot will allow users to self enroll by simply entering their current Windows user name and password.

6. Change Windows passwords for all cardholders

To change Windows passwords for all cardholders at any time, you can follow the description provided in the next section "Set Windows credentials for all members of a group". The password changes will be updated immediately in the card accounts and in Active Directory, if the Program Setting "Synchronize Win Password changes with Active` Directory" is checked.

10.2 Setup to run with more control

This section describes a more "managed" option, where you can have more choices about how you want to handle the system. Card maintenance lifecycle steps, which are also related to Active Directory, are also included.

Assuming that end-users are already known by Active Directory, the Administrator proceeds with the following steps in CardMaker:

1. Specify desired card settings for default user group
2. Import end-user data from Active Directory
3. Issue template card for default user group
4. Save Windows logon entry on template card
5. Assign Windows logon entry to all members of group
6. Set Windows credentials for all members of group
7. Issue ConCERTO LOGON accounts to cards, or allow self-enrollment
8. Reissue lost card
9. Issue cards to subsequent new employees
10. Change passwords for all cardholders

Each step is explained in more detail below. You may also refer to the individual section in this manual for additional information on any of the above topics.

1. Specify desired card settings for default user group

You must first specify the card settings that you want to use as a default, so that the end-users that are imported from Active Directory will automatically be assigned to the default user group. If you have a large number of individuals who will be assigned the same card settings, it is recommended that you use this user group as your default user group - by naming this group for example, "GeneralUser".

> TIP: You can always create a more exclusive user group with different card settings, to be assigned to management personnel, for example. In this case, you would then change the User Group specification of the management individuals after import from Active Directory has been completed, under Card > View/Edit Cardholder.

Continuing for this example with the "GeneralUser" user group, go to Configuration > Card Settings. Specify card

settings as desired and save as "GeneralUser". When prompted if you want to designate file 'GeneralUser.ini' as the Default User Group Card Settings File", click on Yes.

2. Import end-user data from Active Directory

1. Go to Tools > Data Import > Open. Click on the sample file which has been provided, as a template. You will get an error message, since the sample file does not yet contain information which is specific to your installation.
2. Change the DSN or Connection String to your access parameters. In many cases, you just need to change computer name, and domain. Note that a DNS recognizable name is preferable to IP address if you are using SSL.
3. Enter the administrator login User ID and Password that give you privileges to access Active Directory.
4. Click on Connect. After successful connection, click on Select.
5. You may now specify the Field Names that you want to import. If you import the field names as depicted in the image above and specified below, this will be sufficient to ensure a good working relationship between Active Directory and CardMaker:
   Card_ID: (leave blank)
   Cardholder_ID: (leave blank)
   ConCERTOUserName: userPrincipalName (ie, sbeaton@mydomain.com)
   Last_Name: sn
   First_Name: givenName
6. Click on the Save As button to save the data import specifications to file. Save the file with a easily recognizable name, and you can then use this file to execute future imports, or with the Schedule Data Synchronization option, to have data imported on a regular basis.
7. Click on "Import=" if you want to ensure that only end-users who are listed in Active Directory will be listed in CardMaker. Or, click on "Import+" if you want to only add new end-user information to the ConCERTO CardMaker list. See the Data Import section, for additional information.
8. To view the end-users who have been imported into ConCERTO CardMaker, go to Card > View/Edit Cardholder.

3. Issue template card for default user group

You will now create a template card which will enable you to transfer a Windows logon entry to all cardholders in a user group.

1. Go to Card > Issue Card > Add New. Take a card from the card stock and present it to the reader.
2. Ensure that the default user group for the template card is the previously created default card settings file, in the case of our example, "GeneralUser". Then specify the Cardholder ID for the template card as "TemplateGeneralUser", for example.
3. Click on Issue button to issue the template card.

4. Save Windows logon entry on template card

1. Go to Tools > Create Managed Entries. The Logon Manager application will open.
2. Using your template card, create a Windows logon entry under Settings > Logon to Windows, entitled for example "Network logon". Change Permissions as desired, and save.
3. Close ConCERTO LOGON Manager application.

5. Assign Windows logon entry to all members of group

1. Go to Tools > Assign Managed Entries. Click on the Windows logon entry that you just created with your template card, for example "Network logon…"
2. Click on the "Copy to" button, and select the user group that you created - in our example "GeneralUser". Click on the "Paste" button, to paste entry to all end-users in that group.

6. Set Windows credentials for all members of group

In the Assign Managed Entries screen, click on the Credentials button, then click on the "select all" button, to set the Windows logon credentials for all of the end-users in the user group that you created.

Click on the Set Credentials button, and choose the options that best suit your installation. Refer to the table below for

assistance.

Set user name of selected Windows logon entry to value of 'CardholderID'.	**Recommendation:** If you imported end-users from Active Directory, this option can always be selected. **Why:** During import, the 'CardholderID' field in CardMaker is filled from the Windows logon User Name field in Active Directory.
Set to default password. Default password = …	**Recommendation:** Select if you want to specify a default password, for example, if you want to specify a default password for new users that they are required to immediately change. **Why:** Default passwords can be helpful for individuals as well as groups, depending on your needs.
Set to random password.	**Recommendation:** Select if you want ConCERTO LOGON to create a random password for each individual end-user that was selected on the previous screen. **Why:** This option is appropriate for two scenarios: if you will be completely managing the Windows passwords and the end-user will never know his Windows password. Or, if you want to provide each end-user with their Windows password, you can print out a Password Letter for each individual end-user (under Reports).
Do not change password.	**Recommendation:** Select if do not want ConCERTO LOGON to change the Windows password for the selected end-users. **Why:** Selecting this option will not affect the password entry in Active Directory if you have elected to synchronize Windows password changes with Active directory, and will leave the Windows logon password field for each end-user card account blank. This is appropriate, for example, if end-users will be specifying their own Windows logon passwords.

Click on Set Credentials button, to set end-user credentials as specified.

Important Note: If you want a Windows password change to be also immediately synchronized with Active Directory, you must have the "Synchronize Win Password Changes with Directory" option checked under Configuration > Program Settings > LDAP/Active Directory. Otherwise, Windows password changes will never be synched with Active Directory, and you will have to enter changed passwords into Active Directory manually.

7. Issue ConCERTO accounts to cards, or allow self-enrollment

Since the way that you choose to use Active Directory with ConCERTO LOGON may be affected by how you choose to issue cards, this section provides an overview of the whole process. The following scenarios for card issuance or self-enrollment are examined:

- Import end users from Active Directory, and pre-enter Windows logon user name and password into card account.
- Import end users from Active Directory, and pre-enter only Windows logon user name into card account.

These scenarios are provided to help you decide how you want to handle the transition from manual logon to Windows to card-enabled logon to Windows within your organization. The scenarios also include a reference to recommended card settings, and security considerations.

Scenario 1: Import end users from Active Directory, and pre-enter Windows logon user name and password into card account.

Advantages of this option:	▪ Cardholder can use card right away to logon to Windows. ▪ Cardholder never needs to know Windows logon user name or password.

	▪ Administrator can specify if cardholder is allowed to view and/or change Windows user name and password in the template card's Windows logon entry, under the Permissions tab. ▪ Issuing ConCERTO card accounts individually to cardholders (Issuance option 1) provides the highest level of control, or having cardholders self-enroll (Issuance option 2) provides the highest level of convenience.
Issuance option 1: Administrator issues cards	**Issue cards for highest level of control:** ▪ Cardholders bring ID cards to administrator. Administrator issues ConCERTO LOGON account to card by selecting cardholder name from Card > Issue Card option and clicking on Issue button. ▪ Administrator goes to Assign Managed Entries screen, clicks on Credentials button, selects cardholder's Windows logon entry from Managed Entry list, and sets credentials as desired - making sure that any password change is synched with Active Directory. **How it works:** ▪ At end-user PC, cardholder is prompted by ConCERTO LOGON to present his card to logon to Windows. ▪ Upon first use, cardholder is required to change default card PIN. ▪ Card logon to Windows is executed using data in card account. **Recommended card settings:** ▪ Configuration > Card Settings > PIN: Require cardholder to change default PIN with first entry.
Issuance option 2: Cardholders self-enroll	**Self-enroll for best ease of use:** ▪ Cardholders self-enroll with ConCERTO LOGON, using their employee/student ID#, or Windows logon user name, or both, to register their ConCERTO LOGON account. ▪ Before cardholders are instructed to self-enroll, Administrator will generally set Windows credentials for card accounts with current Windows user name and a new random Windows password for the entire group all at once. This can be accomplished as follows: - Announce that cardholders must use cards to logon to Windows the following Monday morning, for example. - The previous Friday night after the workday is over, Administrator goes to Assign Managed Entries screen, clicks Credentials button, and credentials as desired - making sure that any password change is synched with Active Directory. **How it works:** ▪ At end-user PC, cardholder is prompted by ConCERTO LOGON to present his card to logon to Windows. ▪ Upon first use, cardholder is prompted to enter employee/student ID#, or Windows logon user name, or both, to register their ConCERTO LOGON account. ▪ Cardholder is then required to change default card PIN. ▪ Card logon to Windows is executed using data in card account. **Recommended card settings:** ▪ Configuration > Program Settings > Server: Under Self Enrollment options, select desired options, including employee/student ID#, or Windows logon user name, or both, as desired. ▪ Configuration > Card Settings > PIN: Require cardholder to change default PIN with first entry. **Considerations of this option:** ▪ Note that in order to link cardholder with the correct card account, the corresponding employee/student ID#, or Windows logon user name, or both, must already be present in

	the CardMaker cardholder information list under Card > View/Edit Cardholder. If these are both stored in Active Directory, they can be imported into CardMaker. Otherwise, import the Windows logon user name from Active Directory and manually enter the Employee ID# into the CardMaker list, if desired. ▪ Since Windows logon data is already stored in the card account, and cardholders can access it with their card simply by entering information that is known to them, this warning is included in the self-enroll screen: "You must ensure that you enter this information accurately, since this will effectively register your card with your assigned account. If you enter someone else's information, through negligence or with malicious intent, be aware that the system is completely accountable and you will be held responsible."

Scenario 2: Import end users from Active Directory, and pre-enter only Windows logon user name into card account.

Advantages of this option:	▪ Card accounts do not contain the Windows password until the cardholder enters it into card account upon first use. ▪ Cardholders can transition from manual logon to Window to card-enabled logon gradually.
Issuance: Cardholders self-enroll	**Self-enroll for gradual transitioning:** Cardholders self-enroll with ConCERTO LOGON, using their employee/student ID#, or Windows logon user name, or both, to register their ConCERTO LOGON account. **How it works:** ▪ At end-user PC, cardholder is prompted by ConCERTO LOGON to present his card to logon to Windows. ▪ Upon first use, cardholder is prompted to enter employee/student ID#, or Windows logon user name, or both, to register their ConCERTO LOGON account. ▪ Cardholder is also prompted to enter their Windows password on the self-enroll screen. ▪ Cardholder is then required to change default card PIN. ▪ Card logon to Windows is executed using data in card account and entered Windows password. As long as there is only one Windows logon entry in the card account, ConCERTO LOGON will automatically save Windows password to card account, so that no further entry is needed. **Recommended card settings:** ▪ Configuration > Program Settings > Server: Under Self Enrollment options, select desired options, including employee/student ID#, or Windows logon user name, or both, as desired. Specify also that Windows password entry field should be displayed on self-enroll screen. ▪ Configuration > Card Settings > PIN: Require cardholder to change default PIN with first entry. **Considerations of this option:** ▪ Note that in order to link cardholder with the correct card account, the corresponding employee/student ID#, or Windows logon user name, or both, must already be present in the CardMaker cardholder information list under Card > View/Edit Cardholder. If these are both stored in Active Directory, they can be imported into CardMaker. Otherwise, import the Windows logon user name from Active Directory and manually enter the Employee ID# into the CardMaker list, if desired. ▪ Since Windows logon data is already stored in the card account, and cardholders can access it with their card simply by entering information that is known to them, this warning is included in the self-enroll screen:

	"You must ensure that you enter this information accurately, since this will effectively register your card with your assigned account. If you enter someone else's information, through negligence or with malicious intent, be aware that the system is completely accountable and you will be held responsible."

8. Reissue lost card

If a cardholder loses their card, you can re-issue their ConCERTO card account to their new card as described below. In both cases below, Active Directory data will not be affected.

If end-user does not know the card PUK of his previous card or if you prefer to be physically present to re-issue the card:

1. Add lost end-user card to hotlist under Card > Add Card to Hotlist > Report Lost Card, and select lost card from list.
2. Go to Card > Issue Card, and select end-user from list. Present new card to reader and click on Issue Card button.
3. Deliver card to end-user. End-user will use the card PIN from their previous card to access card data.

If end-user knows the card PUK of his previous card:

1. Add lost end-user card to hotlist under Card > Add Card to Hotlist > Report Lost Card, and select lost card from list.
2. Provide end-user with new card.
3. End-user opens ConCERTO LOGON Manager Application. At self enrollment screen, end-user enters required information. When end-user is recognized as a re-issue candidate, he will be prompted to enter PUK from previous card to access card account.

9. Issue cards to subsequent new employees

The suggested procedure for new employees is as follows:

1. Setup new end-user in Active Directory.
2. Go to Tools > Data Import and click on the Open button to open the data import specifications file that you specified with your previous data import, and click on the "Import=" or "Import+" button, as desired. Or, if you have setup the Data Synchronization Scheduler, you can run a preset standard task using the Run Now! button. See the Schedule Data Synchronization section for more information.
3. In Assign Managed Entries screen, assign Windows logon entry from template card to new card account as described above.
4. To enter Windows user name and password into card account, follow description above to set Windows credentials. Remember that if you want a Windows password change to be also immediately synchronized with Active Directory, you must have the "Synchronize Win Password Changes with Directory" option checked under Configuration > Program Settings > LDAP/Active Directory.

10. Change Windows passwords for all cardholders

To change Windows passwords for all cardholders at any time, you can follow the description provided above to "Set Windows credentials for all members of a group". The password changes will be updated immediately in the card accounts.

Important Note: If you want a Windows password change to be also immediately synchronized with Active Directory, you must have the "Synchronize Win Password Changes with Directory" option checked under Configuration > Program Settings > LDAP/Active Directory. Otherwise, Windows password changes will never be synched with Active Directory, and you will have to enter changed passwords into Active Directory manually.

Note also that as long as the "Synchronize Win Password Changes with Directory" option is checked, any Windows password change that you execute in the Assign Managed Entries screen will be synchronized with Active Directory. This includes changes that you make in an individual card account, for example.

10.3 Synchronized Active Directory enrollment

This section describes how to insert entries into the "ConCERTOCfg.ini" file so new end-users are automatically

enrolled in in Active Directory, and accounts of existing users are automatically updated upon card issuance. This feature is especially useful for organizations where end-users don't need to know the Windows logon information that is stored by their card account or organizations where there is a high turnover of end-users, such as schools.

When this feature is used, there is no need to enter new end-users directly into Active Directory. ConCERTO synchronizes Active Directory with the Windows logon data on each card, so that all cards can immediately be used for logon within the network.

For existing users who are already in Active Directory:
ConCERTO LOGON generates a new Windows password and writes it both to the user's Active Directory account (where it "resets" the password), and ConCERTO LOGON account.

For new users:
ConCERTO LOGON creates a new Active Directory account for the user, and generates a new Windows password and writes it both to the user's Active Directory account, and ConCERTO LOGON account. In this case, administrator typically specifies also the following fields in ConCERTO LOGON, which will transfer to the new Active Directory account including:
Cardholder ID: When you enter the user's cardholder ID in combination with the logon domain, it will be written to Active Directory account as Windows "User logon name". Sample format is "55555@user.company.local".
Last Name, First Name: When you enter the user's last name and first name into the corresponding fields, they will be written to Active Directory account.

Note that to use this feature, it is necessary to enter users into ConCERTO first, since access to Active Directory must be controlled. For school installations, this is typically done as follows:

* Existing users are imported into CardMaker from Active Directory (see appropriate section in this manual for assistance. They are then issued ConCERTO LOGON rights at the issuance station at the same time that their ID card is printed.

* New users are entered into CardMaker and issued ConCERTO LOGON rights at the issuance station, ie, students are added to CardMaker at the same time that their ID card is printed.

* When users present their cards to ConCERTO LOGON for the first time, self enrollment is automatically (transparently) accomplished.

To activate this feature, the following three conditions must be met:

1. Using Windows Explorer, go to "Program Files\ConCERTO CardMaker" and double-click (to edit) the "ConCERTOCfg.ini" file. Ensure that the following entries are included, and that they are set to "True":

[PWD.GEN.]
GeneratePwdAtcardIssuance=True

[SELFENROLL]
AutoSelfenroll=True

2. Go to Configuration > Program Settings > Server and confirm that under Self Enrollment, only the following four settings are checked:
- Allow Self Enrollment
- Allow Only for Known Cardholders
- Apply Initial Windows Logon Data
- Self Re-enrollment Only Allowed for Hot-listed Cards

3. Go to Configuration > Program Settings > LDAP/Active Directory and confirm that "Synchronize Win New User and Password Changes" is checked, and that the server connection settings below are correct.

If, for any reason, it should happen that a user's password was not successfully updated in Active Directory, it's easy to update manually. Simply go to Reports > Password Letter and double-click on the Password Letter that was created for the card. Copy/paste the password from the Password Letter into the user's Active Directory account.

Copyright © 2011 SCM Microsystems GmbH

11 Appendix: Using ConCERTO LOGON with Terminal Services

The installation of ConCERTO LOGON for Terminal Services (TS) is basically straight-forward. You can install both ConCERTO LOGON Manager and ConCERTO CardMaker on the same TS server machine for testing, but for production we recommend having Logon Manager on the TS server (= application server) computer and ConCERTO CardMaker on another server computer. There can be several TS application servers, which all communicate with a single ConCERTO CardMaker server. The ConCERTO CardMaker server can optionally be backed up by one or more Fail-Over CardMaker servers.

1. Installation of ConCERTO CardMaker for TS environment:
   Installation of ConCERTO CardMaker for TS environment is no different than non-TS environments.

   Note additional option for TS: as card removal action in Card Settings > WinLogon you can select "Disconnect (TS)", which will trigger disconnect from the TS session when the card is removed from the reader on a terminal.

2. Installation of ConCERTO LOGON Manager for TS environment:
   Typically you install Logon Manager only on the TS server(s), and not on the thin client or terminal computer. If the user will logon not only to the TS session but also to logon to Windows on the client workstation as well, Logon Manager can also be installed on the client computer, but this case is not considered a "standard" installation and might require specialized settings.

Installation on the TS server must be performed directly at the server computer or from a console session with admin rights to the server. A smart card reader driver must be installed on the server. Use a reader driver diagnostic tool to test that reader and driver are available and respond to card insertion. Note that MS Windows will transfer the smart card services from the client computer to the TS server - so when testing the reader driver while connected to the TS server from a console (or TS session), the reader must physically be connected to the client terminal.

After installation of Logon Manager, you must first logon to Windows with a card with Settings > Logon to Windows > "Use card to logon to Windows..." checked. This has to be done directly at the server computer or from a console session with admin rights. This will activate the ConCERTO Gina after reboot of the server. The server is now ready for ConCERTO TS client sessions, as long as the client has card reader and driver installed.

Copyright © 2011 SCM Microsystems GmbH

12 Appendix: Custom Scripts for Card Removal Events

Use the instructions below to make custom scripts for card removal events.

File Name:
"CardRemovalAction_ScriptsDef.ini"
This file is part of the ConCERTO LOGON Manager installation and is located in folder
[Program Files]\ConCERTO LOGON Manager\scripts\

Purpose:
Applies to ConCERTO LOGON Enterprise installations where special actions are to be performed upon card removal. This file can be edited by administrator to include the names of custom script files that are to be executed upon card removal.

Usage:
If this file is present with non-zero entries:
If a custom script is selected to be executed in ConCERTO CardMaker under 'Configuration > Card Settings > WinLogon', and a card with that configuration is used in a ConCERTO LOGON Manager Windows session, the matching custom script file will be executed upon card removal.

Depending on the selected card removal action in Card Settings, ConCERTO LOGON Manager will perform one of the following actions:

Card Settings	Action	Default script name
"No Action"	No action	-
"Logoff User"	Logoff User from Windows	-
"Lock System"	Lock computer	-
"Shutdown System"	Shutdown computer	-
"Logoff User (TSS)"	Logoff User (TSS)	-
"Lock System (TSS)"	Lock computer (TSS)	-
"Disconnect (TSS)"	Disconnect (TSS)	-
"Custom script 001 + Disconnect (TSS)"	Script001* + Disconnect (TSS)	CrdRemAct001.vbs
"Custom script 002"	Script002*	CrdRemAct002.vbs
"Custom script 003"	Script003*	CrdRemAct003.vbs
"Custom script 004"	Script004*	CrdRemAct004.bat
...	...	...
"Custom script 099"	Script099*	CrdRemAct099.bat

Notes:
* = If no matching script file 'Scriptxxx' defined below, the default script file names "CrdRemActxxx.vbs" or "CrdRemActxxx.bat" will be executed.
TSS = Terminal Services Session

If this file is NOT present or has zero entries:
When a card's card settings have been configured for a custom script to be executed upon card removal, the matching default scipt name will be used.

Rules:
Lines that start with a "'" character have been commented out and are ignored.
For example, to activate the first script name re-assignment, delete the "'" comment character in the first position and enter your desired script file name.
Before change:
'Script001="MyCardRemovalAction1.vbs"
After change:
Script001="MyAction1_CloseOpenSessions.vbs"

13 Appendix: Using a Failover Server

The ConCERTO CardMaker server can optionally be backed up by one or more failover ConCERTO CardMaker server(s).

In case of failure of the primary server and with a CardMaker failover server installed, the failover server will automatically take over the functionality of the primary server. End users will be able to logon to their Windows sessions and aplications using ConCERTO LOGON Manager, as long as the configuration and credential data on the CardMaker failover server is current and the server is accessible.

1. Configuration of ConCERTO LOGON Manager client(s) to work with failover servers:
   In order to enable ConCERTO LOGON Manager to connect to the failover CardMaker server in case it can't connect to the primary server, ConCERTO LOGON Manager must know the IP address of the failover server and the sequence in which to attempt to connect to the failover server(s). All server IP addresses of ConCERTO CardMaker servers must be supplied in encrypted form. The encrypted addresses can be obtained by contacting your ConCERTO reseller or the software manufacturer at concerto@scmmicro.com.

   Example A of file "rfip.ini" with NO failover server:
   ```
   [RFCardServer]
   RFCardServerCorpName="XYZ Corporation - ConCERTO Server"
   RFCardServerIP="B6E254234370456A0B068AF7E7EBE1258EAB9AD92E2FFF14"
   RFCardServerPath=/rfserver/rpc.asp
   ```

   Example B of file "rfip.ini" with one failover server:
   ```
   [RFCardServer]
   RFCardServerCorpName="XYZ Corporation - ConCERTO Server"
   RFCardServerIP="B6E254234370456A0B068AF7E7EBE1258EAB9AD92E2FFF14"
   RFCardServerIP2="B6E251234370456A0B067AF7E7EBE125748C40384B70B239"
   RFCardServerPath=/rfserver/rpc.asp
   ```

2. Configuration of ConCERTO CardMaker server to operate as failover server:
   The failover CardMaker server should be installed on the same type of computer with identical or similar configurations as the primary server. It must be ensured that the CardMaker installation on the failover server are always updated to the same version as CardMaker on the primary server.

   In order to ensure that the data on the failover server is current, the data and configuration files of the primary CardMaker server should be backed up to the CardMaker failover server(s) by an automated scheduled procedure. At the minimum, the following files should be kept synchronized:
   ...\Program Files\ConCERTO CardMaker\ConCERTO.ini
   ...\Program Files\ConCERTO CardMaker\CardMaker.ini
   ...\Program Files\ConCERTO CardMaker\PreSelRdrs.ini
   ...\Program Files\ConCERTO CardMaker\data*.mdb
   ...\Program Files\ConCERTO CardMaker\CardSettings*.ini

   The file "rfip.ini" must be set to correct IP address.

   For the above example B, the rfip.ini file for the first failover server would look like this:
   ```
   [RFCardServer]
   RFCardServerCorpName="XYZ Corporation - ConCERTO Server"
   RFCardServerIP="B6E251234370456A0B067AF7E7EBE125748C40384B70B239"
   RFCardServerPath=/rfserver/rpc.asp
   ```

When the rfip.ini files have been set correctly on both client and server computers, the clients will automatically connect to the failover server in case the primary server fails.

Copyright © 2011 SCM Microsystems GmbH

14 Appendix: Configuring Multiple CardMaker Stations

There are three configuration options for networks that require multiple CardMaker stations:

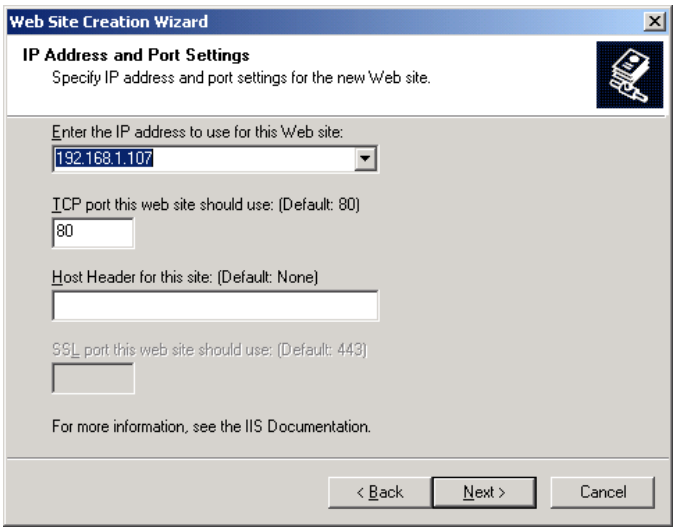
A	**Independent Mode:**	Independent CardMaker stations use individual program settings and maintain separate databases. Although the CardMaker stations are connected over the network, they do not share information. This is the default mode.
B	**Global Mode:**	CardMaker stations linked over a network that share program settings and a database. To set up: Install CardMaker on each desired machine. Connect each station to the same SQL database. Then confirm that in the CardMaker Configuration menu under Local Settings the setting for "SiteID" is the same for all CardMaker stations. For a description of how to install the SQL database, please ask your reseller for the ConCERTO SQL Server Installation Kit.
C	**Mixed Mode:**	CardMaker stations linked over a network that maintain individual program settings but share a database. To set up: Install CardMaker on each desired machine. Connect each station to the same SQL database. Then in the CardMaker Configuration menu under Local Settings, you must specify the setting for "SiteID" giving each CardMaker station a unique site ID. For a description of how to install the SQL database, please ask your reseller for the ConCERTO SQL Server Installation Kit.

Copyright © 2011 SCM Microsystems GmbH

15 Appendix: SSL-Secured Website Setup

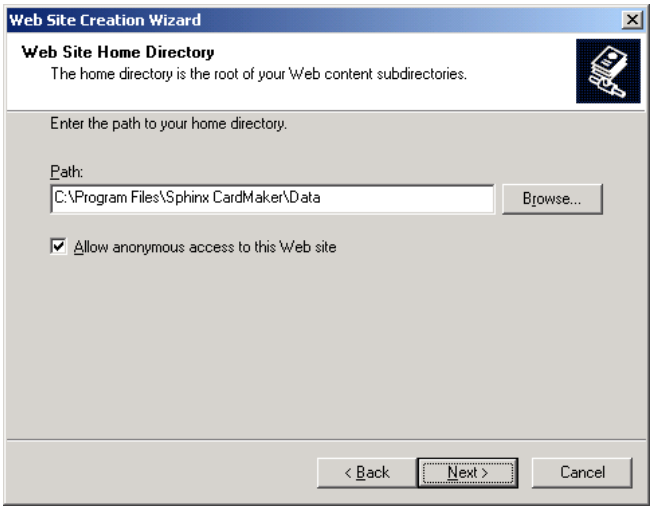
15.1 Open Internet Information Services and Create a Website

3. Right-click on computer icon (with name of your computer).
4. From the menu, select New>Website.
5. Click on Next in the Welcome to the Web Site Creation Wizard screen.
6. For Web Site Description, enter "rfserver".
7. Under IP Address and Port Settings, select the IP address that you would like to assign for ConCERTO CardMaker. (A fixed IP address must have already been assigned to the computer prior to this step.)


Web Site Creation Wizard
IP Address and Port Settings
Specify IP address and port settings for the new Web site.
Enter the IP address to use for this Web site:
192.168.1.107
TCP port this web site should use: (Default: 80)
80
Host Header for this site: (Default: None)
SSL port this web site should use: (Default: 443)
For more information, see the IIS Documentation.
< Back
Next >
Cancel

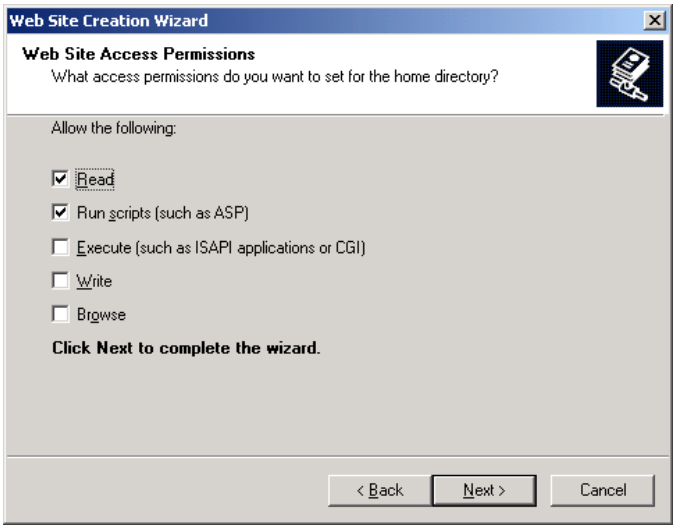
Click on Next to continue

8. Under Web Site Home Directory, click on Browse and select the "data" sub-directory underneath your ConCERTO CardMaker program directory.


Web Site Creation Wizard
Web Site Home Directory
The home directory is the root of your Web content subdirectories.
Enter the path to your home directory.
Path:
C:\Program Files\Sphinx CardMaker\Data
Browse...
Allow anonymous access to this Web site
< Back
Next >
Cancel

Click on Next to continue.

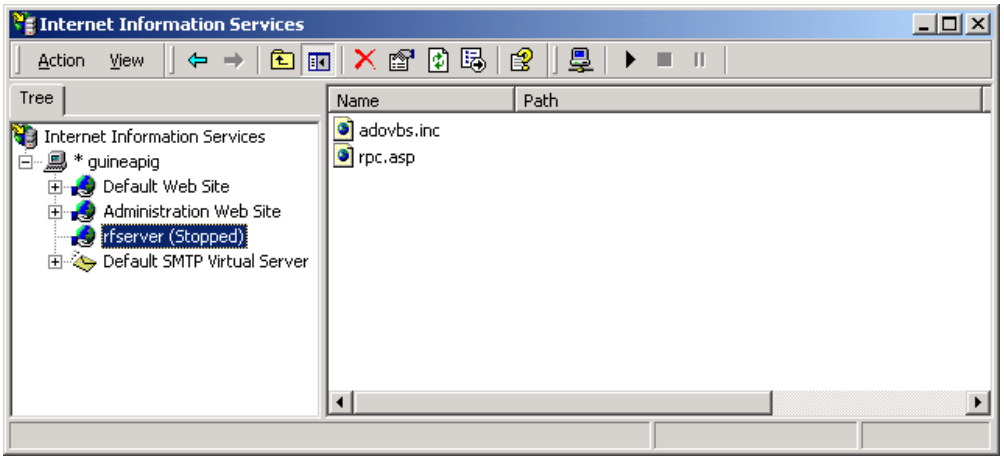
9. Under Web Site Permissions, select "Read" and "Run scripts"


Web Site Creation Wizard
Web Site Access Permissions
What access permissions do you want to set for the home directory?
Allow the following:
Read
Run scripts (such as ASP)
Execute (such as ISAPI applications or CGI)
Write
Browse
Click Next to complete the wizard.
< Back
Next >
Cancel

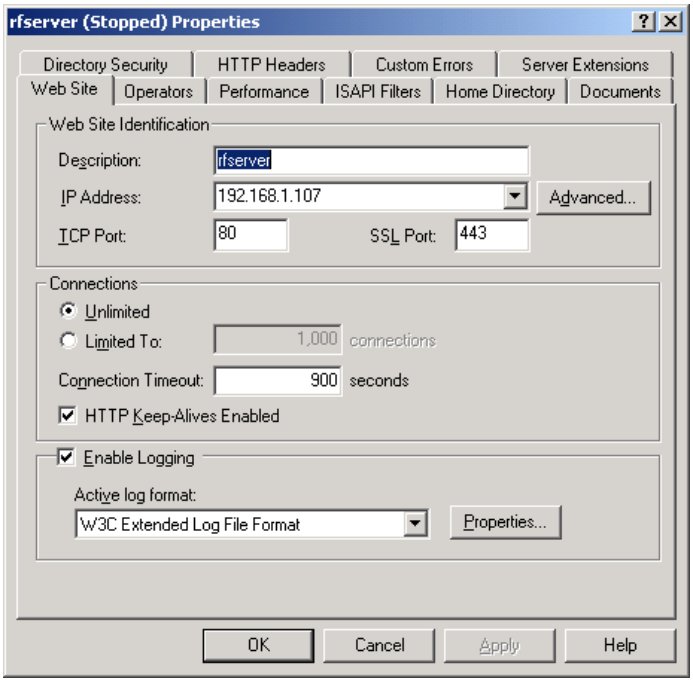
Click on Next to continue

10. On "You have successfully completed the Web Site Creation Wizard", click on Finish to complete.

11. Right-click on "rfserver" and select "properties" from the menu.



12. Enter "443" for SSL Port and click on OK.



15.2 Setup SSL

Follow Microsoft instructions "How To Set Up SSL on a Web Server" MSDN Library to SSL-secure the web site "rfserver".
(http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod30.asp)

16 Appendix: SSL-Secured Client Setup

16.1 Setup of SSL-Secured Client

After having completed the steps in Setup of SSL-Secured Website for ConCERTO CardMaker you must ensure that the Certificate Authority's Certificate is installed on all client computers where ConCERTO LOGON Manager is installed and configured to connect to the CardMaker server.

Follow the Microsoft MSDN Library* steps provided below to verify that the CardMaker SSL secured web service is accessible from a ConCERTO LOGON Manager client computer:

1. Open "Internet Explorer" browser.
2. Enter in the browser's address field: "HTTPS://myWebServer /rpc.asp" and press Enter.
   (replace the sample IP " myWebServer " with the URL or IP address of your CardMaker web service)
3. If the **Security Alert** dialog box, as illustrated in the figure below, is displayed, ConCERTO LOGON Manager will not be able to connect to the CardMaker server. Click **View Certificate** to see the identity of the issuing CA for the Web server certificate. You must install the CA's certificate on the client computer. This is described below in procedure "Install the Certificate Authority's Certificate on the Client Computer."
4. If your SSL-secured CardMaker web service is accessible, you should get the following response:
   "SCM_RpcAspError:CMServer.CardSvr AccessCardSvr Error: no command string supplied."

   Note: If your ConCERTO LOGON Manager client works in server mode during a Windows session but fails during logon to Windows with a card (error message: "can't connect to server"), follow steps 7 - 29 of the procedure "Install the Certificate Authority's Certificate on the Client Computer."

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site s security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

5. Close Internet Explorer.

16.2 Install the Certificate Authority's Certificate on the Client Computer

This procedure installs the issuing CA's certificate on the client computer as a trusted root certificate authority. The client computer must trust the issuing CA in order to accept the server certificate without displaying the **Security Alert** dialog box.

Perform this procedure only if your Web server certificate was issued by a Microsoft Certificate Services CA. Otherwise, if you have the CA's .cer file, go to Step 8. Follow the Microsoft MSDN Library* steps provided below.

1. Start Internet Explorer and browse to http:// *hostname*/certsrv, where *hostname* is the name of the computer where Microsoft Certificate Services that issued the server certificate is located.
2. Click **Retrieve the CA certificate or certificate revocation list**, and then click **Next**.
3. Click **Install this CA certification path**.
4. In the Root Certificate Store dialog box, click Yes.
5. Browse to ConCERTO CardMaker Web service using HTTPS. For example:
6. https://myWebServer/rpc.asp

   The CardMaker Web service error message page should now be correctly displayed by the browser, without a **Security Alert** dialog box (**Figure 1**).

   You have now installed the CA's certificate in your personal trusted root certificate store. To enable ConCERTO LOGON Manager to call the Web service successfully during logon to Windows, you must add the CA's certificate to the computer's trusted root store.

7. Repeat Steps 1 and 2, click Download CA certificate, and then save it to a file on your local computer.
8. Now perform the remaining steps, if you have the CA's .cer certificate file.
9. On the taskbar, click **Start**, and then click **Run**.
10. Type **mmc**, and then click **OK**.
11. On the **Console** menu, click **Add/Remove Snap-in**.
12. Click **Add**.
13. Select **Certificates**, and then click **Add**.
14. Select **Computer account**, and then click **Next**.
15. Select **Local Computer: (the computer this console is running on)**, and then click **Finish**.
16. Click **Close**, and then **OK**.
17. Expand **Certificates (Local Computer)** in the left pane of the MMC snap-in.
18. Expand **Trusted Root Certification Authorities**.
19. Right-click **Certificates**, point to **All Tasks**, and then click **Import**.
20. Click **Next** to move past the **Welcome** dialog box of the Certificate Import Wizard.
21. Enter the path and filename of the CA's .cer file.
22. Click **Next**.
23. Select **Place all certificates in the following store**, and then click **Browse**.
24. Select **Show physical stores**.
25. Expand **Trusted Root Certification Authorities** within the list, and then select **Local Computer**.

26. Click **OK**, click **Next**, and then click **Finish**.
27. Click **OK** to close the confirmation message box.
28. Refresh the view of the **Certificates** folder within the MMC snap-in and confirm that the CA's certificate is listed.
29. Close the MMC snap-in.

* The above information contains procedure descriptions taken from the Microsoft MSDN Library.

17 Appendix: Deactivating Card-Supported Windows Logon

If you want to deactivate the ConCERTO Gina without having to run ConCERTO LOGON Manager, you can use the tool provided in Program Files > ConCERTO LOGON Manger > ResetCardLogon.exe, as displayed below.

Deativate Card-Supported Windows Logon
Your Windows Registry is currently set to the following custom Gina:
Entry location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL
Gina name: NOT FOUND
Removing above registry value from the Windows Registry will deactivate the associated Gina the next time the system is booted.
The original custom GINA uses the entry "odgina.dll" and is active whenever the checkbox "Use card to logon to Windows" in end user application is checked. Should the registry entry show any other custom gina name then this entry should not be deleted, unless you are sure that you want to do this in order to remove any gina from the registry that is chained with this application's odgina.dll.
Note: After deactivation you will need to reboot computer to activate the standard Windows logon behavior. Make sure to reboot before uninstalling or updating the end-user logon application.
Do you want to delete above registry entry?
Yes
Cancel

This tool is useful for example, if your ConCERTO LOGON Manager installation has been corrupted (hard disk crash, virus), and you need to reset the Windows logon.

18 Appendix: Import String Formats

For use with Data Import tool.

String Formats

You can use any of the following characters to create a format expression for strings:

Character	Description
@	Character placeholder. Display a character or a space. If the string has a character in the position where the at symbol (@) appears in the format string, display it; otherwise, display a space in that position. Placeholders are filled from right to left unless there is an exclamation point character (!) in the format string.
&	Character placeholder. Display a character or nothing. If the string has a character in the position where the ampersand (&) appears, display it; otherwise, display nothing. Placeholders are filled from right to left unless there is an exclamation point character (!) in the format string.
<	Force lowercase. Display all characters in lowercase format.
>	Force uppercase. Display all characters in uppercase format.
!	Force left to right fill of placeholders. The default is to fill placeholders from right to left.

Numeric Formats

The following table identifies characters you can use to create user-defined number formats:

Character	Description
None	Display the number with no formatting.
(0)	**Digit placeholder.** Display a digit or a zero. If the expression has a digit in the position where the 0 appears in the format string, display it; otherwise, display a zero in that position. If the number has fewer digits than there are zeros (on either side of the decimal) in the format expression, display leading or trailing zeros. If the number has more digits to the right of the decimal separator than there are zeros to the right of the decimal separator in the format expression, round the number to as many decimal places as there are zeros. If the number has more digits to the left of the decimal separator than there are zeros to the left of the decimal separator in the format expression, display the extra digits without modification.
(#)	Digit placeholder. Display a digit or nothing. If the expression has a digit in the position where the # appears in the format string, display it; otherwise, display nothing in that position. This symbol works like the 0 digit placeholder, except that leading and trailing zeros aren't displayed if the number has the same or fewer digits than there are # characters on either side of the decimal separator in the format expression.
(.)	Decimal placeholder. In some locales, a comma is used as the decimal separator. The decimal placeholder determines how many digits are displayed to the left and right of the decimal separator. If the format expression contains only number signs to the left of this symbol, numbers smaller than 1 begin with a decimal separator. To display a leading zero displayed with fractional numbers, use 0 as the first digit placeholder to the left of the decimal separator. The actual character used as a decimal placeholder in the formatted output depends on the Number Format recognized by your system.
(%)	Percentage placeholder. The expression is multiplied by 100. The percent character (**%**) is inserted in the position where it appears in the format string.
(,)	Thousand separator. In some locales, a period is used as a thousand separator. The thousand separator separates thousands from hundreds within a number that has four or more places to the left of the decimal separator. Standard use of the thousand separator is specified if the format contains a thousand separator surrounded by digit placeholders (**0** or **#**). Two adjacent thousand separators or a thousand separator immediately to the left of the decimal separator (whether or not a decimal is specified) means "scale the number by dividing it by 1000, rounding as needed." For example, you can use the format string "##0,," to represent 100 million as 100. Numbers smaller than 1 million are displayed as 0. Two adjacent thousand separators in any position other than immediately to the left of the decimal separator are treated simply as specifying the use of a thousand separator. The actual character used as the thousand separator in the formatted output depends on the Number Format recognized by your system.
(:)	Time separator. In some locales, other characters may be used to represent the time separator. The time

	separator separates hours, minutes, and seconds when time values are formatted. The actual character used as the time separator in formatted output is determined by your system settings.
(/)	Date Separator. In some locales, other characters may be used to represent the date separator. The date separator separates the day, month, and year when date values are formatted. The actual character used as the date separator in formatted output is determined by your system settings.
(E- E+ e- e+)	Scientific format. If the format expression contains at least one digit placeholder (**0** or **#**) to the right of E-, E+, e-, or e+, the number is displayed in scientific format and E or e is inserted between the number and its exponent. The number of digit placeholders to the right determines the number of digits in the exponent. Use E- or e- to place a minus sign next to negative exponents. Use E+ or e+ to place a minus sign next to negative exponents and a plus sign next to positive exponents.
- + $ ( )	Display a literal character. To display a character other than one of those listed, precede it with a backslash (\) or enclose it in double quotation marks (" ").
(\)	Display the next character in the format string. To display a character that has special meaning as a literal character, precede it with a backslash (\). The backslash itself isn't displayed. Using a backslash is the same as enclosing the next character in double quotation marks. To display a backslash, use two backslashes (\\). Examples of characters that can't be displayed as literal characters are the date-formatting and time-formatting characters (a, c, d, h, m, n, p, q, s, t, w, y, / and :), the numeric-formatting characters (#, 0, %, E, e, comma, and period), and the string-formatting characters (@, &, <, >, and !).
("ABC")	Display the string inside the double quotation marks (" "). To include a string in ***format*** from within code, you must use **Chr(**34**)** to enclose the text (34 is the character code for a quotation mark (")).

Date Formats

The following table identifies characters you can use to create user-defined date/time formats:

Character	Description
(:)	Time separator. In some locales, other characters may be used to represent the time separator. The time separator separates hours, minutes, and seconds when time values are formatted. The actual character used as the time separator in formatted output is determined by your system settings.
(/)	Date Separator. In some locales, other characters may be used to represent the date separator. The date separator separates the day, month, and year when date values are formatted. The actual character used as the date separator in formatted output is determined by your system settings.
c	Display the date as ddddd and display the time as ttttt, in that order. Display only date information if there is no fractional part to the date serial number; display only time information if there is no integer portion.
d	Display the day as a number without a leading zero (1 – 31).
dd	Display the day as a number with a leading zero (01 – 31).
ddd	Display the day as an abbreviation (Sun – Sat).
dddd	Display the day as a full name (Sunday – Saturday).
ddddd	Display the date as a complete date (including day, month, and year), formatted according to your system's short date format setting. The default short date format is m/d/yy.
dddddd	Display a date serial number as a complete date (including day, month, and year) formatted according to the long date setting recognized by your system. The default long date format is mmmm dd, yyyy.
w	Display the day of the week as a number (1 for Sunday through 7 for Saturday).
ww	Display the week of the year as a number (1 – 54).
m	Display the month as a number without a leading zero (1 – 12). If m immediately follows h or hh, the minute rather than the month is displayed.
mm	Display the month as a number with a leading zero (01 – 12). If m immediately follows h or hh, the minute rather than the month is displayed.
mmm	Display the month as an abbreviation (Jan – Dec).
mmmm	Display the month as a full month name (January – December).
q	Display the quarter of the year as a number (1 – 4).
y	Display the day of the year as a number (1 – 366).
yy	Display the year as a 2-digit number (00 – 99).
yyyy	Display the year as a 4-digit number (100 – 9999).
h	Display the hour as a number without leading zeros (0 – 23).
Hh	Display the hour as a number with leading zeros (00 – 23).

N	Display the minute as a number without leading zeros (0 – 59).
Nn	Display the minute as a number with leading zeros (00 – 59).
S	Display the second as a number without leading zeros (0 – 59).
Ss	Display the second as a number with leading zeros (00 – 59).
t t t t t	Display a time as a complete time (including hour, minute, and second), formatted using the time separator defined by the time format recognized by your system. A leading zero is displayed if the leading zero option is selected and the time is before 10:00 A.M. or P.M. The default time format is h:mm:ss.
AM/PM	Use the 12-hour clock and display an uppercase AM with any hour before noon; display an uppercase PM with any hour between noon and 11:59 P.M.
am/pm	Use the 12-hour clock and display a lowercase AM with any hour before noon; display a lowercase PM with any hour between noon and 11:59 P.M.
A/P	Use the 12-hour clock and display an uppercase A with any hour before noon; display an uppercase P with any hour between noon and 11:59 P.M.
a/p	Use the 12-hour clock and display a lowercase A with any hour before noon; display a lowercase P with any hour between noon and 11:59 P.M.
AMPM	Use the 12-hour clock and display the AM string literals as defined by your system with any hour before noon; display the PM string literal as defined by your system with any hour between noon and 11:59 P.M. AMPM can be either uppercase or lowercase, but the case of the string displayed matches the string as defined by your system settings. The default format is AM/PM.

Copyright © 2011 SCM Microsystems GmbH

19 Appendix: Active Recorder Applications

Administrator can change an .ini file in ConCERTO LOGON Manager installations, if they want to specify that the Auto-Recorder for Windows application logons will only offer to record applications which are predefined.

Then, when the "Enable Auto-Recorder for Windows application logons" option is activated under "Settings - General", the Auto-Recorder will only offer to record applications which are listed in the .ini file.

To change the "RecorderActiveApplicationList.ini" file, go to
"C:\ProgramFiles\ConCERTO LOGON Manager"
Double-click on
"RecorderActiveApplicationList.ini"
to open the file and follow the instructions provided in the file, as shown below.

```
'*********************************************************************************************
'File Name:
'       "RecorderActiveApplicationList.ini"
'       This file is part of the ConCERTO LOGON Manager installation.
'Purpose:
'       File can be edited by user / Administrator to include the Window Title of applications
'       that should automatically be recognized by ConCERTO to bring up the Auto-Record prompt.

'
'Usage:
'  If this file is present:
'    Non-web Windows applications with an entry form that have at least one password field
'    and have a Window title that matches a title in the list below will be available for the
'    ConCERTO "Auto-Record" function.
'
'  If this file is NOT present:
'    Non-web Windows applications with an entry form that have at least one password field
'    will be available for the ConCERTO "Auto-Record" function.
'
'Rules:
'  Entries for Window title can contain "*" a wildcard charater as the first character,
'  last character, or first and last character.
'  In order to be recognized as active, the entries below must start with "AppWinTitle" without
'  the "'" comment character.  Entries must be sequentially numbered.  Entries shown below are
'  for demonstration purposes only and must be replaced by customized entries in order to
'  activate this feature.
'*********************************************************************************************


[ApplicationWindowTitles]
'AppWinTitle1="*Logon Test Application"
'AppWinTitle2="*My Application - Window Title - (to be recognized by ConCERTO Auto-Record function)"
'AppWinTitle3="*Password Application"
...
```

20 Appendix: Best Practice for Web /App Design

ConCERTO LOGON Manager should not have any problems with recording most standard websites and applications. The following conditions, however, could pose a problem and should be avoided:

Web Sites

To understand the issues facing the ConCERTO LOGON recorder, it is important to understand what information ConCERTO LOGON stores about a web site.

- The URL of the top page (displayed in the browsers address bar). ConCERTO LOGON looks for the URL when auto-fill is enabled. For space reasons, ConCERTO LOGON does not store URLs of sub-frames. Consider that URLs can be very long.
- Frame name (if present).
- Form name.
- Input field name.
- Input field type (text or password, all other fields are ignored).
- And finally, input field value.

Potential Problems

- Frames
  ConCERTO LOGON recognizes pages by their top parent URL. ConCERTO LOGON needs this information to navigate to the site when the user activates the entry in ConCERTO LOGON. A link in a frame, however, will only change the URL in the frame, the top URL stays the same. Problems occur when the linked page contains another form with the same name as the previous form on the previous page, and if that form contains input fields with the same names as the previous input fields. Since both pages would meet ConCERTO LOGON's selection criteria, it would fill both forms with the same credentials.

  Auto-Submit should be avoided with forms in frames. Fortunately, frames are more and more disappearing from modern web sites.

- Self-modifying Pages
  Self-modifying pages pose a similar problem as described for frames. Depending on certain input parameters, a page using the same URL could display a form with the same name but with different input fields.

  How do you recognize a self-modifying page? The URL does not change when you navigate through the page, but contents, especially of forms, change.

  Auto- Submit should be avoided with self-modifying pages.

- Multiple Forms With No Names
  ConCERTO LOGON distinguishes by form name, and if there are multiple forms with no names on a page, then ConCERTO LOGON enumerates the forms in the order of their appearance. If the order changes in a new design, then ConCERTO LOGON would fill the wrong form.

  Auto-Submit should be avoided on pages with multiple forms.

Version Changes

As a general safeguard, auto-submit should not be used on web sites since their layout can change at any time. Having auto-submit turned off will give the user the opportunity to verify that the site is still good and genuine.

Windows Applications

ConCERTO stores the following information about a Windows application:

- The window title that is displayed in the title bar. ConCERTO LOGON looks for the title when the auto-fill feature is enabled.
- Fully qualified path and name of the application executable. ConCERTO LOGON needs this information to start the application when the user activates the entry in ConCERTO LOGON.
- Window ID of the input field. If not available (for example, applications created with Borland compilers) ConCERTO LOGON enumerates the windows in the order of their appearance.

Copyright © 2011 SCM Microsystems GmbH

- Input field type (text or password)
- And finally, input field value

Potential Problems

When the user clicks or navigates to a new input field, ConCERTO LOGON first gathers information about the window:

- Window handle
- Class name – some compilers use descriptive names such as "TextBox" or "ComboBox" while others use non-descriptive names such as "#31212".
- Attributes – a bit combination of values representing window properties such as 'is visible', 'is password', etc. Passwords will be only placed in fields that have the password attribute set.

Problems can arise with:

- Non-descriptive Class Names
  ConCERTO LOGON is unable to determine the type of window if the class name does not describe its nature such as "textbox" or "button".
- Missing Attributes
  If the class name didn't yield any clues, then ConCERTO LOGON looks at attributes to further determine the type of the window. However, this method is not always reliable. For example, a window may have an attribute of 'visible', but is obscured by other windows or is placed outside of the visible screen area, so to the user it is not visible. Well-designed programs should not have this problem, but there can be exceptions (for example, Outlook calendar which includes an 'invisible' password window). ConCERTO LOGON maintains an allow list with those applications that ConCERTO tracks for Auto-Recorder and Auto-Fill.
- Logon Dialog In Same Window as Main Application
  Auto-Recorder automatically ends recording when the logon window disappeared. If an application displays the logon dialog in the same window as the main application, then ConCERTO LOGON is unable to detect the end of the recording session. The user needs to press the OK to end the recording and return to the ConCERTO LOGON entry screen.
- Keystroke Recording In Password Fields
  ConCERTO LOGON is able to read the text out of regular text windows; however, the operating system does not allow this for password windows. ConCERTO LOGON uses a keystroke recorder to record entries in password fields. The following should be avoided in a password field:
  - Backspace or delete key
  - Cursor keys
  - Repositioning of the cursor with the mouse

  If there is any doubt about the quality of the password recording, the user should verify its contents by showing it in the clear in the Enter Logon Info screen.

Version Changes

It is fairly safe to permit auto-submit on selected Windows applications. When a new release is installed, the user should turn auto-submit off and verify that the logon entry is still valid for the new release.